LAS TOP 100 HERRAMIENTAS DE SEGURIDAD



NEX IT SPECIALIST #30

BEST SECURITY TOOLS EVER

- BEST SECURITY TOOLS EVER -

WWW.NEXWEB.COM.AR
ISSN 1668-5423
9 771668 542003 00030
Correo Argentino FRANQUEO A PAGAR Cta. 10195



DIRECTOR
- Dr. Carlos Osvaldo Rodriguez

PROPIETARIOS
- Editorial Poulbert S.R.L.

RESPONSABLE DE CONTENIDOS
- Dr. Carlos Osvaldo Rodríguez

DIRECTOR COMERCIAL
- Ulises Román Mauro
umauro@nexweb.com.ar

COORDINACIÓN EDITORIAL
- Alejandro Perakes
- Carlos Rodríguez

SENIOR SECURITY EDITOR
- Carlos Vaughn O'Connor

EDITORES TÉCNICOS
- María Delia Cardenal
- Thomas Hughes
redaccion@nexweb.com.ar

DISEÑO Y COMUNICACIÓN VISUAL
- DCV Esteban Báez
- Carlos Rodríguez Bontempi

DISTRIBUCIÓN
distribucion@nexweb.com.ar

ASISTENTE COMERCIAL
- Martín Guaglianone

SUSCRIPCIONES
- Maximiliano Sala
- Andrés Vázquez
suscripciones@nexweb.com.ar

PREIMPRESIÓN E IMPRESIÓN
IPESA Magallanes 1315. Cap. Fed.
Tel 4303-2305/10

DISTRIBUCIÓN
Distribución en Capital Federal y Gran Buenos Aires: Huesca Distribuidora de Publicaciones S.A. Aristóbulo del Valle 1556/58. C1295ADH - Capital Federal Argentina. (www.distribuidorahuesca.com.ar)
Distribuidora en Interior: DGP Distribuidora General de Publicaciones S.A. Alvarado 2118/56 1290 Capital Federal - Argentina
NEX IT Revista de Networking y Programación
Registro de la propiedad Intelectual en trámite leg número 3038 ISSN 1668-5423
Dirección: Av. Corrientes 531 P 1
C1043AAF - Capital Federal
Tel: +54 (11) 5031-2287

Si desea escribir para nosotros, enviar un e-mail a:
articulos@nexweb.com.ar



Nota del Editor

"Si conoce su enemigo y se conoce a sí mismo, no debe temer por el resultado de cientos de batallas. Si se conoce a sí mismo, pero NO a su enemigo, por cada victoria obtenida sufrirá una derrota. Si no se conoce al enemigo ni a sí mismo, sucumbirá en todas las batallas"

El arte de la guerra, Sun Tzu

Entendiendo al enemigo
Conocer a nuestro enemigo es tan complejo como conocerse uno mismo. A veces los administradores conocen a su enemigo solo a través de "su idea" de él. Muchas veces esa idea nada tiene que ver con la realidad.
Por ejemplo, en las películas se muestra cómo se accede a una computadora mediante la rotura de una llave de encriptación. La película muestra al atacante tipeando la clave, adivinándola y lo resuelve en segundos. O escribe un programa con una interfase gráfica con grandes números donde puede crackear cada carácter de la clave uno por uno. Estas simulaciones son totalmente irreales y nada tienen que ver con los conceptos matemáticos que gobiernan las metodologías de encriptación.

¿Cómo hacemos entonces para defendernos?
La respuesta es: conocer. Para poder mejorar la seguridad y protegernos debemos conocer bien las modalidades usadas por los hackers. Los hackers cuentan con innumerables herramientas y metodologías que no podemos desconocer. Ellos, debido a su naturaleza se reinventan continuamente y a sus técnicas.
El profesional de seguridad deberá por tanto conocer muy profundamente el ámbito de ataque y la filosofía de los atacantes de modo de poder ayudar a las empresas respecto de su seguridad. Deberá crear medidas concretas haciendo menos vulnerables la infraestructura IT de las empresas.

En esta tarea de "conocer" han aparecido un gran número de libros, conferencias, eventos divulgando las técnicas de hacking en la búsqueda de mostrar cómo opera el enemigo.
Sabemos que esta temática es muy vigente, de importancia y que apasiona a nuestros lectores.

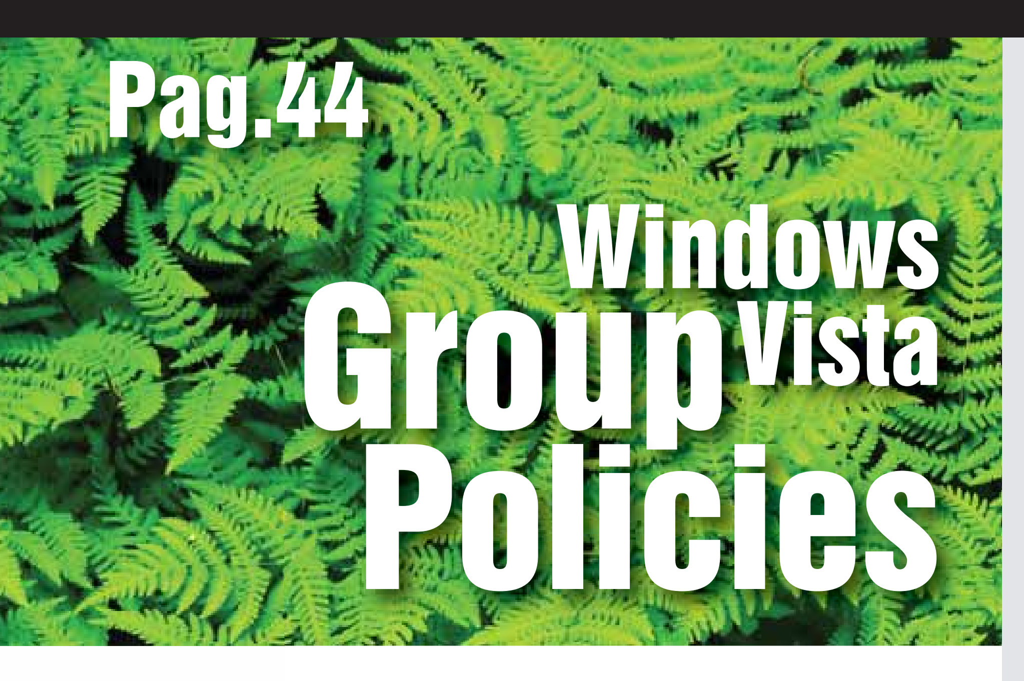
Bajo el título "Best Security Tools Ever" (Las Mejores Herramientas de Seguridad que Jamás han Existido) les describiremos:
#1 Las Herramientas (NEX #30)
#2 Las Metodologías de quiénes las usan (en un próximo número)

Desde esta Editorial no queremos dejar de destacar como bibliografía indispensable en este tema la serie de libros cuyos autores pertenecen a una de las empresas más prestigiosas de Seguridad Informática (Foundstone Inc.: www.foundstone.com): www.hackingexposed.com. Casi todos han sido traducidos al español y editados en McGraw Hill/InterAmericana de España (lamentablemente las traducciones son —paupérrimas!!! Excepto el de "Hackers en Linux").
También invitamos a conocer a las instituciones privadas y gubernamentales que le han dado marco a toda una serie de actividades educativas y de divulgación a la seguridad informática: el SANS Institute (www.sans.org), el ICS2 (www.ics2.com) creadora de la prestigiosa certificación CISSP, The International Council of Electronic Commerce Consultants (EC-Council®) (http://www.eccouncil.org), The Institute for Security and Open Methodologies (ISECOM) www.isecom.org donde se definen estándares en test de seguridad y testeo de la integridad de los negocios

Como siempre, "NEX IT Specialist" incluye otros temas y sus series.

Y no dejen de contactarnos a ***redaccion@nexweb.com.ar***

SUMARIO



Microsoft ISA Server 2006





Best Security Tools Pag.11

De una encuesta realizada por Fyodor a 20.000 hackers que utilizan Nmap, con el propósito de que describieran sus herramientas de seguridad favoritas, respondieron 3.243 personas. Los interesados en el tema de seguridad encontrarán información de utilidad en la lista y podrán también conocer productos con los que todavía no están familiarizados. Dada la característica especial de los consultados, las respuestas tendrán una leve orientación hacia los ataques más que a la defensa.

SE REALIZÓ EL SNOOP UPDATE 06



Se llevó a cabo la segunda edición del Snoop Update, el encuentro para desarrolladores de software con el objetivo de brindar conocimiento sobre herramientas, metodologías y buenas prácticas para facilitar la inserción de nuevas tecnologías en las empresas. El evento, llevado a cabo en el complejo Paseo La Plaza, logró una convocatoria de 1.500 personas inscriptas a las distintas actividades, y ofreció valiosas exposiciones de especialistas acerca de temas de alta tecnología.
El Update ha sido una actividad totalmente gratuita destinada a arquitectos, líderes de desarrollo y desarrolladores profesionales interesados en conocer las nuevas herramientas comerciales y de Open Source para el desarrollo de software.



En esta edición se destacó el espíritu de apertura que inspira el Update para construir puentes entre todo el mercado.
"Este es un aporte para toda la industria del software y los servicios en tecnología informática, que necesita de la formación y actualización permanente de la gente para poder mantener el crecimiento de estos últimos años", señaló Gustavo Guaragna, CEO de Snoop Consulting.
En paralelo se desarrolló el Update 4 CIOs, un ciclo de charlas exclusivo para directivos de informática, que contó con la participación de ejecutivos destacados de la industria de tecnología de la información.
El encuentro Update '06 contó con el apoyo de Oracle e IBM como Sponsors Diamond, Microsoft y Datamarkets como Sponsors Platinum, Red Hat y SAP como Sponsors Gold, y Suivant, Business Objects y Microsiga como Sponsors Silver. Contó también con el aporte de destacadas entidades adherentes y media sponsors.



Para más información visite: *www.snoopconsulting.com*



UN AÑO MÁS DE EXPOCOMM

Luego de 4 días, más de 24.000 asistentes y 173 empresas expositoras, finalizó la décimo cuarta edición de Expocomm Argentina, el evento dedicado a las telecomunicaciones y a la tecnología de la información.
Esta última edición de Expocomm, llevada a cabo en la Rural entre el 3 y 6 de octubre, contó con un total de 16 mil metros cuadrados brutos divididos en tres pabellones. A diferencia del año pasado, los organizadores E.J. Krause & Associates, Reed Exhibitions Argentina y la Cámara de Informática y Comunicaciones de la República Argentina (CICOMRA) decidieron agregar un nuevo pabellón y diferentes áreas para que tanto los expositores como los asistentes pudieran maximizar su presencia en el evento.
En total se registraron 173 empresas expositoras divididas en ocho rubros: Comunicaciones, Soluciones de Seguridad, E-commerce, Networking, Storage, Consultores e Integradores y Herramientas de Desarrollo. Entre ellas Telefónica de Argentina, Blackberry, Sony, Dattatec.com, Global Software, la Embajada de los Estados Unidos, CTI Movil, Terra, MercadoLibre.com, LG Electronics, Movistar, Probattery y Telecom entre otras.
Además se organizó un Seminario de Tecnología y Mercado a la que asistieron 550 personas y cubrió los temas de mayor relevancia en materia de avances e innovaciones en informática y telecomunicaciones. Contaron con la participación de reconocidos especialistas nacionales e internacionales, entre los que se destacan los CEOs de las empresas líderes del sector, quienes en Paneles Temáticos y Presentaciones Magistrales de KeyNote Speakers, expusieron su visión.
La Revista NEX IT Specialist también estuvo presente en el evento de la tecnología y la comunicación. Con un stand en el pabellón Canadá (de color amarillo) más de 18.000 personas pasaron por el stand y probaron suerte con la rueda de la fortuna. Para la próxima edición de Expocomm, planeada entre el 9 y el 12 de octubre de 2007, ya fue vendido el 75 por ciento de la exposición y además se planea agregarle al predio 4.800 metros cuadrados.
Para más información no dude en visitar: *www.expocomm.com.ar*

CALENDARIO DE EVENTOS IT EN ARGENTINA PARA EL 2006

Fecha	OCTUBRE	Informes
26 y 27	**Jornadas Nacionales AGSI 2006 -** Hotel Sheraton Libertador	www.worktec.com.ar
	NOVIEMBRE	
2	**Jornadas Trabajo IT 2 -** Sheraton Libertador.	www.trabajoit.com.ar
2 al 5	**AES - Argentina Electronic Show -** La Rural, Predio Ferial de Buenos Aires.	www.aeshow.com.ar/es_services_contact_us
6	**Soluciones de Seguridad open Source** - Buenos Aires Sheraton Hotel	www.cybsec.com/capacitacion
10 y 11	**GNU/Linux y Software Libre** - UADE - Buenos Aires	www.cafeconf.org
13 al 16	**Cisco Networkers Solution Forum 2006 -** Hotel Hilton Buenos Aires	www.cisco.com/ar/networkers
14 y 15	**Consecri-Consetic 2006 -** Sheraton Libertador.	www.consetic.com.ar / www.consecri.com.ar
-	**2do Congreso Nacional de Estudiantes de Sistemas y Tecnologías de la Información**	www.worktec.com.ar - info@worktec.com.ar

Si desea ver su evento IT publicado en esta sección, por favor háganos llegar la información respectiva a: eventos@nexweb.com.ar

Top 100 Best Security Tools

De una encuesta realizada por Fyodor a 20.000 hackers que utilizan Nmap, con el propósito de que describieran sus herramientas de seguridad favoritas, respondieron 3.243 personas. Los interesados en el tema de seguridad encontrarán información de utilidad en la lista y podrán también conocer productos con los que todavía no están familiarizados. Dada la característica especial de los consultados, las respuestas tendrán una leve orientación hacia los ataques más que a la defensa.
Más que describirlas en este orden las agruparemos por temáticas.

Del 1 al 100 en la Lista de Fyodor (no se incluye Nmap)

1 Nessus
2 Wireshark
3 Snort
4 Netcat
5 Metasploit Framework
6 Hping2
7 Kismet
8 Tcpdump
9 Cain y Abel
10 John the Ripper
11 Ettercap
12 Nikto
13 Ping/telnet/dig/traceroute/whois/netstat
14 OpenSSH / PuTTY / SSH
15 THC Hydra
16 Paros proxy
17 Dsniff
18 NetStumbler
19 THC Amap
20 GFI LANguard
21 Aircrack
22 Superscan
23 Netfilter
24 Sysinternals
25 Retina
26 Perl / Python / Ruby
27 L0phtcrack
28 Scapy
29 Sam Spade
30 GnuPG / PGP
31 Airsnort
32 BackTrack
33 P0f
34 Google
35 WebScarab
36 Ntop
37 Tripwire
38 Ngrep
39 Nbtscan
40 WebInspect
41 OpenSSL
42 Xprobe2
43 EtherApe
44 Core Impact
45 IDA Pro
46 SolarWinds
47 Pwdump
48 LSoF
49 RainbowCrack
50 Firewalk
51 Angry IP Scanner
52 RKHunter
53 Ike-scan
54 Arpwatch
55 KisMAC
56 OSSEC HIDS
57 Openbsd PF
58 Nemesis
59 Tor
60 Knoppix
61 ISS Internet Scanner
62 Fport
63 chkrootkit
64 SPIKE Proxy
65 OpenBSD
66 Yersinia
67 Nagios
68 Fragroute/Fragrouter
69 X-scan
70 Whisker/libwhisker
71 Socat
72 Sara
73 QualysGuard
74 ClamAV
75 cheops / cheops-ng
76 Burpsuite
77 Brutus
78 Unicornscan
79 Stunnel
80 Honeyd
81 Fping
82 BASE
83 Argus
84 Wikto
85 Sguil
86 Scanrand
87 IP Filter
88 Canvas
89 VMware
90 Tcptraceroute
91 SAINT
92 OpenVPN
93 OllyDbg
94 Helix
95 Bastille
96 Acunetix Web Vulnerability Scanner
97 TrueCrypt
98 Watchfire AppScan
99 N-Stealth
100 MBSA

Scanning y

NMap

No existe página más prestigiosa que insecure.org. En ella, Fyodor desarrolla Nmap, la herramienta más importante para el experto en seguridad informática.

Introducción

Aplicando la técnica de footprinting se puede obtener una lista de direcciones IP correspondientes a hosts y redes usando los utilitarios whois y nslookup. Estas herramientas nos permiten obtener información, entre otras cosas, sobre rangos de direcciones IP, servidores DNS y servidores de e-Mail. Con esta información en nuestro poder, ya es posible determinar qué sistemas están "vivos" (encendidos) y alcanzables desde internet utilizando una variedad de herramientas que incluyen ping sweeps (barridos de ping), port scans (escaneos de puertos), detección de Sistemas Operativos y automated discovery (descubrimiento automático).

Ping Sweeps

Uno de los pasos más importantes en el trazado de un mapa esquemático de una red es realizar un barrido de ping sobre rangos de direcciones IP y/o bloques de red para determinar cuales sistemas están "vivos". Este paso se realiza con herramientas que permiten hacer la misma tarea que el rudimentario ping, es decir, enviar un ICMP Echo (Tipo 8) al posible destinatario y esperar obtener un ICMP Echo_Reply (tipo 0), determinando así que el posible destinatario está "vivo".

Aunque existen muchas herramientas disponibles en el mercado, en este artículo nos concentraremos en el uso de nmap, una poderosísima herramienta desarrollada por Fyodor (http://www.insecure.org/nmap/). En la Figura 1 vemos la sintaxis para realizar un barrido de direcciones IP utilizando el protocolo ICMP.

El modificador –s permite determinar el tipo de escaneo que se va a realizar (en la Figura 1, la P adicional indica a nmap que haga un ping scan); las direcciones IP de los posibles destinatarios se pueden especificar individualmente o utilizando rangos en cualquiera de los octetos (como en la Figura 1), también se pueden especificar bloques de red (usando por ejemplo: 192.168.0.0/24 ó 192.168.0-12.0/25).

Cuando se hace un barrido de direcciones IP utilizando el protocolo ICMP, hay que hacer todo lo posible por evitar las direcciones de broadcast (difusión), debido a que estas direcciones tienden a producir DoS (Denial of Service-Negación de Servicio).

El primer problema que se puede presentar, al

```
woody:~# nmap -sP 192.168.0.1-254

Starting nmap 3.55 ( http://www.insecure.org/nmap/ )
Host 192.168.0.1 appears to be up.
Host 192.168.0.2 appears to be up.
Host 192.168.0.3 appears to be up.
Host 192.168.0.4 appears to be up.
Host 192.168.0.5 appears to be up.
Host 192.168.0.7 appears to be up.
Host 192.168.0.8 appears to be up.
Host 192.168.0.11 appears to be up.
Host 192.168.0.21 appears to be up.
Host 192.168.0.41 appears to be up.
Host 192.168.0.51 appears to be up.
Host 192.168.0.123 appears to be up.
Host woody (192.168.0.210) appears to be up.
Nmap run completed -- 254 IP addresses (13 hosts up)
woody:~#
```

Fig.1 Resultado de ICMP ping sweep

hacer un barrido de direcciones IP utilizando el protocolo ICMP, es que este protocolo esté bloqueado en un router o firewall en el borde de una DMZ (De-Militarized Zone-Zona Desmilitarizada). Aquí es necesario hacer un barrido de direcciones utilizando otro protocolo y/o evaluando ciertos puertos conocidos de los posibles destinatarios del barrido. En la Figura 2 vemos la sintaxis para realizar un barrido de direcciones IP sin utilizar el protocolo ICMP.

El modificador –s permite determinar el tipo de escaneo que se va a realizar (en la Figura 2, la P adicional indica a nmap que haga un ping scan); pero el modificador PT80 le dice a nmap que haga un TCP probe scan. Así, utilizando el protocolo TCP sobre el puerto 80, se logra que el barrido supere un posible router y/o firewall debido a que muy probablemente el tráfico sobre el puerto 80 del protocolo TCP este permitido.

Como se puede ver, esta técnica es muy efectiva para superar el escollo del bloqueo del tráfico ICMP. También vale la pena reintentar el mismo rango de direcciones utilizando diferentes puertos de protocolos conocidos, por ejemplo: FTP (21) SMTP (25), POP3 (110), RPCBIND (111), IMAP (143), MSRPC (135).

```
woody:~# nmap -sP -PT80 192.168.0.1-254

Starting nmap 3.55 ( http://www.insecure.org/nmap/ )
Host 192.168.0.1 appears to be up.
Host 192.168.0.2 appears to be up.
Host 192.168.0.3 appears to be up.
Host 192.168.0.4 appears to be up.
Host 192.168.0.5 appears to be up.
Host 192.168.0.7 appears to be up.
Host 192.168.0.8 appears to be up.
Host 192.168.0.12 appears to be up.
Host 192.168.0.21 appears to be up.
Host 192.168.0.31 appears to be up.
Host 192.168.0.41 appears to be up.
Host woody (192.168.0.210) appears to be up.
Nmap run completed -- 254 IP addresses (12 hosts up)
woody:~#
```

Fig.2 Resultado de TCP probe

¿Qué es Nmap?

"Network Mapper" es una herramienta Open Source para exploración de redes y auditoría de seguridad. Se diseñó para escanear rápidamente redes de gran escala, aunque funciona muy bien aplicadas a host individuales. Usa los paquetes IP de manera novedosa para determinar qué hosts están disponibles en la red, qué servicios (nombre de la aplicación y su versión) ofrecen esos hosts, qué sistemas operativos (y sus versiones) están empleando, qué tipo de filtros/firewalls están en uso, y muchas características más. NMap puede correrse en la mayoría de las arquitecturas y se puede emplear tanto en versiones de consola como gráficas. NMap es software libre, disponible con todo código bajo la licencia GNU/GPL.

¿Quién es Fyodor?

Se trata de un hacker (definido por él como "quien se divierte jugando con las computadoras y empujando al hardware y software a sus límites") que tiene interés en la seguridad, las redes y la criptografía. Estos temas se superponen pero son esenciales para la seguridad de las redes públicas como es Internet.

Su actividad favorita es programar y aún sabiendo muchos lenguajes la mayoría de su trabajo lo hace en C/C++ o Perl. Se siente cómodo en máquinas corriendo bajo UNIX, especialmente en sistemas open source. Su opinión es que estas plataformas son muy poderosas, pueden redistribuirse libremente y vienen con una colección muy grande de software de utilidad. La disponibilidad del código fuente lo hace más seguros y más fáciles de utilizar y comprender. Su escaner de seguridad NMap ahora corre bajo Windows y por ello se ha esforzado en aprender lo básico de ese ambiente de programación.

Como muchos hackers le gusta leer. Se inspiró en el autor ruso Fyodor Dostoevsky para elegir su "handel" (seudónimo).



Ping Seeps - Contramedidas

El proceso de detección de un Ping Sweep es crucial para determinar si va a ocurrir un ataque, cuándo va a ocurrir y quién lo va a realizar. El principal método de detección de un Ping Sweep es utilizar un NIDS (Network-based Intrusion Detection System-Sistema de Detección de Intrusos basado en Red).

Mientras que la detección de los Ping Sweeps es crítica, la prevención también hará una contribución substancial. Es recomendable que evalúe el tipo de tráfico ICMP que permite circular en su red. Recuerde que existen 18 tipos distintos de tráfico ICMP, Echo y Echo_Reply son sólo 2 de ellos.

Port Scanning

Hasta aquí hemos visto como se puede determinar qué sistemas están "vivos", utilizando las técnicas de Ping Sweep o de TCP Probe Scanning. Habiendo recolectado esta información, ya es posible hacer un Port Scanning (Escaneo de Puertos) sobre cada equipo/sistema individual. Port Scanning consiste en establecer conexiones TCP y UDP a un equipo de destino (una posible "víctima") para establecer qué servicios están en ejecución o en estado Listening (escuchando). Los servicios activos que estén escuchando pueden permitir el acceso no autorizado a usuarios no deseados. Estos usuarios podrían lograr acceso a servidores que están mal configurados o que tienen instaladas versiones de aplicaciones que tienen vulnerabilidades conocidas.

Port Scanning - Tipos de Scan

Existen varios tipos de escaneo de puertos, dando una perspectiva distinta de cómo detectar servicios y/o aplicaciones. Asimismo, los diferentes tecnicismos de cada uno de ellos permitirá hacer los escaneos con un mayor o menor grado de sigilo.

- TCP connect scan: este tipo de scan se conecta al puerto de destino haciendo un Three-Way Handshake completo.
- TCP SYN scan: esta técnica es conocida también como "half-open scanning", debido a que solamente se envía un paquete con el flag SYN a la "víctima", si esta responde con un flag SYN/ACK el puerto esta escuchando, si responde con un flag RST/ACK el puerto esta cerrado. Para evitar el Three-Way Handshaking, se envía un paquete con el flag RST/ACK, y así se logra que la "víctima" no registre una conexión.
- TCP FYN scan: con esta técnica se envía un paquete con el flag FIN a la "víctima", y esta debe responder un paquete con el flag RST para los puertos que estén cerrados.
- TCP Xmas Tree scan: con esta técnica se envía un paquete con los flags FIN, URG y PUSH a la "víctima", y esta debe responder un paquete con el flag RST para los puertos que estén cerrados.
- TCP Null scan: con esta técnica se envía un paquete que tiene todos los flags apagados a la "víctima", y esta debe responder un paquete con el flag RST para los puertos que estén cerrados.
- UDP scan: con esta técnica se envía un paquete a un puerto específico de la "víctima", y esta debe responder un paquete ICMP Port_Unreachable para los puertos que estén cerrados. Los únicos problemas de esta técnica son: su falta de fiabilidad y su baja performance.

En la Figura 3 podemos ver a nmap haciendo un TCP SYN scan sobre uno de los destinos "vivos" de la red.

El modificador –s permite determinar el tipo de escaneo que se va a realizar (en la Figura 3, la S adicional indica a nmap que haga un TCP SYN scan); es posible especificar el FQDN de la "victima", pero es preferible usar su dirección IP.

Las direcciones IP de los posibles destinatarios se pueden especificar individualmente o utilizando rangos en cualquiera de los octetos (como en la Figuras 1 y 2, pero hay que hacer todo lo posible por evitar las direcciones de broadcast).

Para los demás tipos de escaneo es necesario usar una T (TCP connect scan), F (TCP FIN scan), X (TCP Xmas Tree scan), N (TCP Null scan) o U (UDP scan).

Si agregamos el modificador V (resultando en –sSV) nmap tratará de informarnos de la versión de la aplicación y/o servicio que está escuchando en ese puerto.

```
woody:~# nmap -sS 192.168.0.4

Starting nmap 3.55 ( http://www.insecure.org/nmap/ )
Interesting ports on 192.168.0.4:
(The 1648 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1025/tcp open  NFS-or-IIS
1400/tcp open  cadkey-tablet
1433/tcp open  ms-sql-s
3372/tcp open  msdtc
3389/tcp open  ms-term-serv
MAC Address: 00:08:54:05:F5:32 (Netronix)

Nmap run completed -- 1 IP address (1 host up)
woody:~#
```

Fig.3 Resultado de TCP SYN

Port Scanning - Contramedidas

El principal método de detección de un Port Scanning es utilizar un HIDS (Host-based Intrusion Detection System-Sistema de Detección de Intrusos basado en Sistemas Individuales). También es posible utilizar un NIDS con su placa de red configurada en modo promiscuo.

De la misma manera que la prevención ayudaba a evitar los Ping Sweeps, la correcta configuración y mantenimiento de los routers y/o firewalls hará que sea más difícil que un intruso conozca los puertos/servicios/aplicaciones abiertos en los sistemas que se estén asegurando.

Detección de SO

Si prestamos atención a las respuestas que dio nmap al TCP SYN scan, podemos interpretar esos datos y deducir, siguiendo algunas premisas conocidas, que la máquina "víctima" tiene alguna clase de sistema operativo Windows (debido a los puertos 135 y 139 abiertos). Pero muchas veces, los puertos abiertos en un sistema no son faciles de deducir y producen incertidumbre.

Aquí entra en juego nuevamente nmap que nos permite mediante el modificador –O identificar de acuerdo al fingerprint del stack TCP cuál es el sistema operativo de la "víctima". Vemos en la Figuras 4 un ejemplo de detección de sistema operativo.

```
woody:~# nmap -O 192.168.0.21

Starting nmap 3.55 ( http://www.insecure.org/nmap/ )
Interesting ports on 192.168.0.21:
(The 1643 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
9/tcp     open  discard
13/tcp    open  daytime
  :
901/tcp   open  samba-swat
933/tcp   open  unknown
9999/tcp open  abyss
MAC Address: 00:08:54:06:16:DB (Netronix)
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.6.4 (x86)

Nmap run completed -- 1 IP address (1 host up)
woody:~#
```

Fig.4 Resultado de detección de SO

También existen otras herramientas disponibles para la detección de sistemas operativos, un ejemplo muy conocido es QueSo (www.apostols.org/projectz/). Es importante recordar que QueSo no es un Port Scanner, solamente hace detección de sistema operativo a través del puerto TCP:80.

Detección de SO - Contramedidas

Debido a que el proceso de detección de Sistema Operativo de una máquina "víctima" es esencialmente un análisis del fingerprint del stack TCP, las herramientas para evitar esta técnica son las mismas que para evitar un Port Scanning: HIDSs y NIDSs.

Descubrimiento automático

Existen herramientas muy completas diseñadas para englobar varias funcionalidades en el scanning. Mencionaremos dos: I) Cheops (http://www.marko.net/cheops/) que engloba usando una interfaz gráfica a ping, traceroute, port scanning, y scanning de SOs. II) Tkined (parte del paquete Scotty, http://wwwhome.cs.utwente.nl/~schoenw/scotty/)

Conclusión

Hemos visto hasta aquí las principales herramientas y técnicas de scanning existentes, la información que es posible obtener y la utilidad de dicha información. Como postre a nuestro banquete de herramientas y técnicas, sólo queda nombrar una herramienta que permite hacer todas estas tareas en conjunto y desde una única interfaz: Nessus (www.nessus.org), una herramienta que consta de 2 partes, el Server esta disponible sólo para plataformas Unix y/o Linux y el cliente esta disponible para cualquier plataforma. El cliente funciona en modo gráfico.

Historia del Hacking

cDc: Cult of the Dead Cow

Durante el verano de 1998 miembros de "The L0pht", una de las organizaciones de hackers más interesantes, notorias y productivas fueron invitados a Washington DC, USA, a testificar ante el Senado de los Estados Unidos. Los miembros Space Rogue, Mudge, Brian Oblivion, Dildog, Silicosis, Kingpin y Weld Pond habían ganado tanta notoriedad que el gobierno americano los había convocado para escucharlos.

Quizás una de las características más curiosas de su aparición en el Senado fue verlos con traje. Normalmente su atuendo se asemejaba más a una banda de punks. Fue aquí donde manifestaron al Senado que podrían (si lo deseaban) hacer caer Internet en media hora.

Este quizás fue el punto culminante en la trayectoria de "The L0pht" y sus miembros. Su prestigio estaba muy alto lo que llevó a capitales de riesgo a fusionar a "The L0pht Heavy Industries" con el start up de seguridad informática @Stake (www.atstake.com). Los miembros de "The L0pht" componen la división R&D (investigación y desarrollo) de @Stake.

La historia no terminó allí. Fueron invitados por el presidente Bill Clinton a formar parte del Consejo de Seguridad en Internet. Interesante fue como el presidente se dirigió a ellos por sus nombres "handle" (nombre con los que actúan como hackers) en lugar de sus nombres verdaderos.

La historia de "The L0pht" y sus miembros está muy ligada a otra institución de hackers: cDc (Cult of the Dead Cow). Conozcamos la historia de cDc y su relación con "The L0pht".

El Culto de la Vaca Muerta

El Culto de la Vaca Muerta (Cult of the Dead Cow - cDc) [1] es una organización hacker de alto perfil fundada en 1984 en Lubbock, Texas. Esta organización es muy famosa por su lanzamiento del Back Orifice, en 1998, y Back Orifice 2000, en 1999. Durante los años 80, la cDc se hizo conocida a través de los BBSs por sus newsletters, que continúan produciendo hoy en día.

En diciembre de 1990, el miembro **Drunkfux (dFx)** creó la primera convención moderna de hackers: Ocón. Realizada generalmente en Houston, Texas, que fue la primera convención de hackers que invitó a periodistas y legisladores. En total, dFx realizó cinco HoHoCons.

El 7 de enero de 1999, la cDc se unió con una coalición internacional de hackers para denunciar una llamada a la "cyberguerra" contra los gobiernos de China y de Iraq. Más adelante ese año la cDc creó "Hacktivismo", un grupo independiente dedicado a la creación de tecnología anti-censura en pos del cumplimiento de los derechos humanos en Internet. En búsqueda de uno de sus objetivos llamado "Dominación Global por Saturación Mediática" (Global Domination Through Media Saturation). A través de los años, los miembros de la cDc han concedido entrevistas a importantes periódicos, revistas impresas, sitios de noticias en línea y programas de noticias internacionales de televisión. En febrero de 2000, la cDc era el tema principal de un documental de 11 minutos titulado "Disinformation".



¿Qué es The L0pht?

La cDc tiene lazos con "The L0pht" en calidad de miembro común. The L0pht [2], además de ser un taller en Boston, es el nombre del grupo de hackers que lo hicieron famoso. A ocho años de su creación el grupo realizó su "open house", una fiesta de muy difícil acceso. Brian Oblivion, uno de los fundadores de The L0pht, comenzó a armar esta fiesta con una lista de canciones organizadas en su laptop. Debe haber sido una de las pocas veces en que se vio a un DJ trabajar sobre una pila de libros de computación (Criptografía Aplicada, El Hackeo Expuesto, Seguridad de Redes bajo NT, etc.). La noche fue dedicada a rejuntar viejos amigos y a cerrar un capítulo en la evolución de The L0pht.

Aunque se conocen 4 fundadores iniciales (*Brian Oblivion, Count Zero [Zero], Golgo 13 [Golgo] y White Knight [WK]*), había un quinto integrante. Sin esta gran personalidad The L0pht nunca habría sido lo que fue. Y ese gran talento, ese elemento estelar del underground de Boston es la esposa de Brian Oblivion. La señora Oblivion es fabricante de sombreros. Cuando su negocio comenzó a ampliarse más allá de las limitaciones de su hogar ella encontró un loft para dirigir su negocio. Y mientras se establecía allí, decidió mudar la "creciente colección de hardware" de Brian (por no decir la "pila de placas y gabinetes" que cualquier esposa descartaría gustosa de su casa) de su departamento al loft. Otros tres compartieron el mismo destino. *Zero, Golgo* y *WK* tenían más cosas de las que el espacio en sus casas les permitía. De a poco The L0pht fue abandonando el caos y se fue armando prolijamente con toda la tecnología de la que disponían. Este grupo terminó conformando, sin saberlo, el taller hacker más grande del mundo.

Al mismo tiempo que The L0pht, había otros grupos, como Messiah Village y Newhackcity; todos poblados con el mismo tipo de hackers: jóvenes, brillantes e interesantes. Había hackers con poca educación formal en informática. Algunos fueron a la universidad y estudiaron antropología o música. Otros nunca hicieron algo más allá de la secundaria. Pero lo que todos tenían en común era la capacidad para aislar las aplicaciones de las computadoras que manejan y luego volverlas a juntar de maneras más poderosas y personalizadas.

La formación de quienes fundaron The L0pht se desarrolló en los años 80, en la época de los BBSs. Estas conformaron una red de conexiones dial up a lo largo de Norteamérica y Europa. Se comunicaban en g-files (o "text-files") y estos archivos contendrían el código para los exploits de telefonía y computación, historias fantásticas, letras de canciones, y el más creativo arte ASCII jamás capturado.

En el epicentro de este movimiento estaba el Culto De La Vaca Muerta. Dos de los fundadores originales de The L0pht son miembros de la cDc, al igual que dos actuales miembros, Mudge y Dildog. Aunque la cDc y The L0pht son dos organizaciones distintas y se-

paradas, han compartido miembros y se han influenciado muchísimo. The L0pht fue lanzado hacia el final de la era BBS con el nacimiento de la WWW. Por años hosteó el sitio original del Culto De La Vaca Muerta, tanto como algunas de las colecciones más extraordinarias de contenido sobre hacking, phracking y anarquía en la corta historia de la WWW. No había chico en el mundo interesado en hacking que no haya entrado alguna vez (sino varias) al sitio Web de The L0pht para ingresar a un mundo de aprendizaje que le cambiaría la vida para siempre.

Todo el tiempo el equipo de The L0pht trabajó en proyectos de hacking. La mayoría del trabajo giró alrededor del newsletter de seguridad, y con el tiempo comenzaron a montar un arsenal de tecnología sobre la que probarían sus invenciones y hazañas. The L0pht comenzó a publicar sus resultados generalmente como "L0pht Advisories"; detallando los códigos que, luego de su revisión, ellos consideraban que necesitaban una corrección. Estos "Advisories" han hecho mucho por la fama de The L0pht. Los hackers han tendido siempre a la apertura y no a la oscuridad. Si se descubren exploits, estos son expuestos así todos pueden conocerlos, y no solo los que quieren hacer daño.

Proyecto BO2K

Back Oriffice 2000 (conocido como BO2K) es una herramienta de administración remota de redes. Puede correrse en modo "stealth", una característica común en las aplicaciones de este tipo. Esto significa que un usuario no sabría que su máquina es administrada externamente. Además de esto, *Dildog*, quien programó esta aplicación, lo hizo de forma tal que resultó ser un programa muy pequeño; lo suficientemente pequeño como para ser enviado como adjunto en un e-mail; como para ser abierto, instalado y tenerlo funcionando en un momento; y como para pasar inadvertido. La cDc lanzó esta aplicación con mucha fanfarria, haciendo una gran campaña publicitaria.

El lanzamiento de BO2K demostró que podrían ofrecer al público una aplicación de código abierto, gratuita, mejor que cualquier otra en el mercado, y que actuaba como una llamada de atención al público. BO2K se puede programar para funcionar como troyano (un programa que funciona en la máquina de los usuarios sin el conocimiento del mismo). Esta aplicación, más que cualquier otra iniciativa, creó conciencia pública sobre los peligros de los troyanos, aunque algunos aprovecharon la ocasión para entretenerse "manejándole" la PC a algún compañero de oficina.

Este es el tipo de trabajo que The L0pht y cDc han realizado desde su inicio. Buscando los defectos, haciéndolos conocidos y creando herramientas que refuercen la red para convertirla en un lugar más seguro. Han estudiado productos de *vendors* (empresas) de software y hardware y los han forzado a corregir los errores y lanzar mejores productos. Los miembros de The L0pht también se han comunicado extensamente con las diferentes publicaciones referentes a seguridad en Internet. *Space Rogue*, otro miembro de The L0pht, lanzó la "Red de Noticias del Hacker" [3], uno de los pocos lugares en la Web que cubre ediciones para hackers con mucha credibilidad.

Referencias

[1] *www.cultdeadcow.com*
[2] *www.l0pht.org*
[3] *www.spacerogue.net*

Wireless Tools

#1 | Kismet

Un poderoso sniffer para redes inalámbricas

Poderoso sniffer para redes inalámbricas. Es un sniffer de red sobre el protocolo 802.11b, a y g. Es capaz de realizar sniffing sobre la mayoría de las tarjetas inalámbricas, detección automática de bloques de IP vía paquetes UDP, ARP y DHCP, loggin de paquetes bajo criptografía débil y con archivos de paquetes compatibles con Ethereal y tcpdump.

En la lista general: #7

También clasificado como: packet sniffers

#2 | NetStumler

Sniffer gratuito de 802.11 para Windows

Sniffer de redes wireless no intensivo pues identifica a los access points que están realizando broadcast de sus nombres (SSID), además permite identificar la dirección MAC del dispositivo. Trabaja sobre plataforma PC Windows.

En la lista general: #18

También clasificada como: packet sniffers

#3 | Aircrack

La herramienta más rápida de crackeo de WEP/WPA

Herramienta de crakeo para 802.11a/b/g WEP y WPA. Puede atacar 1 ó 2 redes utilizando métodos avanzados de criptografía o a través de la fuerza bruta.

En la lista general: #21

También clasificado como: password crackers

#4 | Airsnort

Herramienta de crackeo del cifrado WEP de 802.11.

Herramienta para redes inalámbricas capaz de recuperar llaves de encriptación. Opera monitoreando la red en forma pasiva y reuniendo una suficiente cantidad de paquetes hasta "adivinar" la clave.En la lista general: #31

También clasificada como: password crackers

#5 | KisMAC

Stumbler inalámbrico para Mac OS X

Ofrece mucha de las aplicaciones de Kismet pero a través de una base de códigos enteramente diferente.

En la lista general: #55

También clasificada como: packet sniffers

Vulnerability Exploitation Tools

1 | Metasploit Framework

Hackea el planeta

Metasploit es una avanzada plataforma "Open Source", diseñada específicamente con el objetivo de potenciar y agilizar, el desarrollo, testeo y utilización de exploits.

En la lista general: #5

2 | Core Impact

Herramienta de testeo de penetración automática

No es barato pero es considerado una de las más poderosas herramientas de explotación disponibles. Si Core Impact le resulta muy caro, puede optar por Canvas que es más barato, o por el libre Metasploit Framework.

En la lista general: #44

Otra Clasificación: vulnerability scanners

3 | Canvas

Extensa plataforma de Exploitation

Canvas es una herramienta no-libre de exploración de vulnerabilidades. Incluye más de 150 exploits y es más barato que Core Impact. También se puede comprar el opcional Visual Sploit Plugin.

En la lista general: #88

Application Specific Scanners

#1 | THC Amap

Escáner de identificación de aplicaciones

Es un escáner poderoso que prueba cada puerto buscando identificar aplicaciones y servicios en lugar de confiar en un mapeo de puertos estático.

En la lista general: #19

#2 | Nbtscan

Recolecta información de NetBIOS de redes de Windows

Escanea redes IP en busca de información de nombres de NetBIOS. Envía pedidos de "status" de NetBIOS a cada dirección en un rango provisto por el usuario y lista la información recibida de manera humanamente legible. Por cada host que responde, se lista su dirección, nombre de NetBIOS, nombre de usuario con sesión iniciada en la máquina ("logged in"), y dirección de MAC.

En la lista general: #39

#3 | Ike-scan

Detector y escáner de VPN

Ike-scan es un exploit que transporta las características en el Internet Key Exchange (IKE), el mecanismo usado por VPN para establecer una conexión entre un servidor y un cliente remoto.

En la lista general: #53

#4 | SPIKE Proxy

Cracking de HTTP

Es un proxy de HTTP "open source" que sirve para encontrar fallas de seguridad en sitios web y es parte del Spike Application Testing Suite. y soporta detección de inyección de SQL automatizada, crawling de sitios web, uso de fuerza bruta en formularios de entrada, detección de overflow, y detección de acceso a directorios que debieran estar fuera de los límites del sitio de web ("directory traversal").

En la lista general: #64

Rootkit Detectors

#1 | Sysinternals

Extensiva colección de poderosas utilidades de ventana

Sysinternals prove pequeñas utilidades de ventana que son útiles para hackeos de bajo nivel. Algunas son gratis y hasta incluyen el código de fuente, mientras que otras no.

En la lista general: #24

#2 | Tripwire

El abuelo de las herramientas de comprobación de integridad de archivos

Tripwire es una herramienta que ayuda a administradores y usuarios de sistemas monitoreando alguna posible modificación en algún set de archivos. Si se usa regularmente en los archivos de sistema Tripwire puede notificar a los administradores del sistema, si algún archivo fue modificado o reemplazado, para que se puedan tomar medidas de control de daños a tiempo. Una version "Open Source" para Linux está disponible de manera gratuita en Tripwire.Org.

En la lista general: #37

#3 | RKHunter

Infaltable detector de seguridad

Rkhunter es una muy buena utilidad para detectar trojanos, rootkits, y otros problemas de seguridad.

En la lista general: #52

#4 | chkrootkit

Localizador de rootkits

chkrootkit es un programa que permite localizar rootkits, realizando múltiples pruebas en las que busca entre los binarios ficheros modificados por dicho rootkit. Funciona en sistemas operativos BSD, FreeBSD, OpenBSD, Linux, y Solaris.

En la lista general: #63

SNORT bajo WINDOWS

El NIDS (Network Intrusion Detection System) OPEN SOPURCE ahora corriendo bajo Windows

Infinidad de paquetes con información atraviesan a gran velocidad las redes de computadoras. Algunos fueron diseñados con malas intenciones; pueden pasar los firewalls y las defensas perimetrales ingresando y dañando nuestro sistema.
Seguramente, ha experimentado algún ataque con SQL SLAMMER, CODE RED, NIMDA y MSBlaster. Todos estos programas maliciosos utilizan protocolos confiables: HTTP o SMB/CIFS de Microsoft para alcanzar a realizar su maligna función. La opción NO es bloquear esos protocolos. Las organizaciones emplean los llamados IDS (Intrusion Detection Systems, Sistemas de Detección de Intrusos). En particular, aquellos que monitorean las redes: los NIDS (Network IDS).
Es posible encontrar en el mercado excelentes NIDS. Sus precios y capacidades son variados. Generalizando son todos buenos y cumplen su función con eficacia. Existe además una versión de fuente abierta (Open Source) denominada SNORT. A diferencia de lo que ocurre generalmente esta aplicación Open Source del mundo Unix like (Linux, OpenBSD) corre en Sistemas Operativos de Microsoft. Y se trata de un producto eficaz.

SNORT, el sistema de detección de intrusos de la fuente libre

“SNORT es un sistema de detección de intrusos de tipo liviano. Es capaz de llevar a cabo en tiempos reales un análisis del tráfico y logonear un paquete en trabajos de red IP. Está preparado para hacer análisis protocolizado buscar contenidos y unirlos y puede detectar variedad de ataque y pruebas como neutralizar sobreflujo, escanear port steath, ataques CGI, pruebas SMB, intentos de huella digital y mucho más”.
“Snort usa un lenguaje de reglas flexibles para describir el tráfico que debe recolectar o pasar, así como una maquinaria de detección que utiliza una arquitectura modular de conexión. Snort también tiene capacidad de alerta de tiempo real, incorporando mecanismos de alerta para syslog, un archivo específico de usuario, una conexión UNIX, o mensajes de Winpop a los clientes Windows utilizando el smbclient de Samba”.
“Tiene 3 usos primarios. Puede ser usado directamente como un sniffer de paquetes similar a tcpdump, un logger de paquetes (de utilidad para el trabajo de red de tráfico debugging, etc) o como detector de intrusión en el sistema”.

-Extractado de snort.org

La Historia de SNORT

SNORT fue desarrollado alrededor de 1998 por Martin Roesch (el fundador de Sourcefire, http://www.sourcefire.com/snort.html) y ofertado con licencia GPL/GNU. Se trata de una aplicación ampliamente probada, realizada con contribuciones de la comunidad Open Source. La versión actual puede llevar a cabo en tiempo real un análisis del tráfico IP y su registro (loggin) de redes con Fast Ethernet y Gigabit Ethrnet. Snort fue llevado a la plataforma Windows (Win32) por Michael Davis. Chris Reid ha continuado esta tarea y actualmente SNORT para Windows está presentado como un ejecutable de muy sencilla implementación.

Recursos para SNORT bajo WINDOWS

• SNORT corre bajo Windows desde WIN2k professional y posteriores (XP, Win2K Server, Windows Server 2003)
• Por lo menos una placa de red. Quizás la mejor opción es tener dos placas de red, una conectada a la red a monitorear y otra a nuestra red de producción.
• No se requiere licencia ya que es una aplicación OpenSource.
• No son necesarios demasiados recurso computacionales. El programa es muy eficiente. Por ejemplo SNORT con 900 MHz y

Intrusion Detection Systems

1 | Snort

Un sistema de detección de intrusiones libre
Sistema de detección de intrusos (IDS) de software libre. Es liviano, capaz de realizar análisis de tráfico en tiempo real y registro de los paquetes IP de las redes. Puede realizar análisis de protocolo, búsqueda/correspondencia de contenidos y puede detectar una variedad de ataques y pruebas.
En la lista general: #3

2 | OSSEC HIDS

Sistema de detección de intrusos Open Source
Plataforma de análisis integrada, capaz de responder activamente y cuenta con alertas temporales. También es usualmente utilizado como solución de SEM/SIM.
En la lista general: #56

3 | Fragroute/Fragrouter

Detección de intrusos
Intercepta, modifica, y reescribe el tráfico de salida. Entre sus características, se encuentra un lenguaje de reglas simple para retrasar, duplicar, descartar, fragmentar, superponer, imprimir, reordenar, segmentar y especificar source-routing.
En la lista general: #68

4 | BASE

El motor básico de análisis y seguridad
BASE es un motor de análisis para buscar y procesar una base de eventos de seguridad generados por IDSs, firewalls y una herramienta de monitoreo de network.
En la lista general: #82

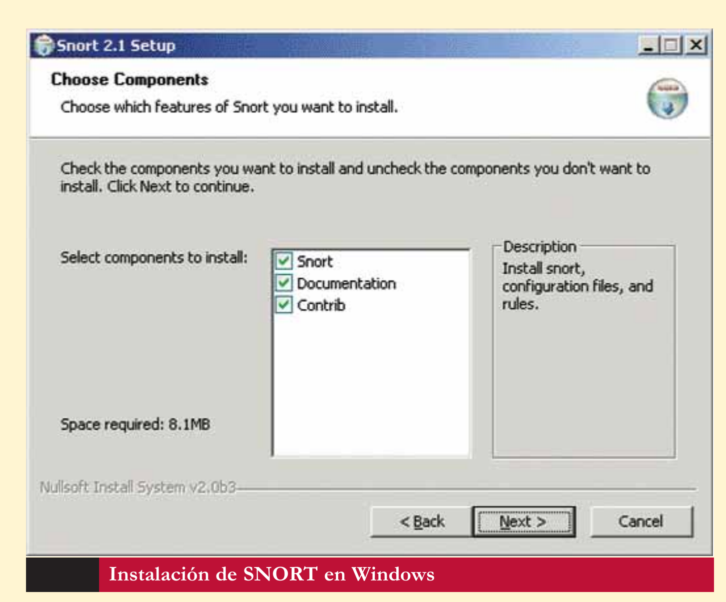
5 | Seagull

La consola de análisis para el monitoreo de seguridad de network
El principal componente de Sguil es un GUI intuitivo que provee eventos de tiempo real de Snort. Además incluye componentes que facilitan la práctica de Monitoreo de Seguridad de Network.
En la lista general: #85

```
C:\>snort -l c:\snort\log -c\snort\etc\snort.conf -A console
Running in IDS mode
Log directory = c:\snort\log
Initializing Network Interface \Device\Packet_NdisWanIp
OpenPcap() device \Device\Packet_NdisWanIp network lookup:
        The operation completed successfully.
        --== Initializing Snort ==--
Initializing Output Plugins!
Decoding Ethernet on interface \Device\Packet_NdisWanIp
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file \snort\etc\snort.conf

++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
,-----------[Flow Config]----------------------
| Stats Interval:  0
| Hash Method:     2
...
      IIS Unicode Map: GLOBAL IIS UNICODE MAP CONFIG
      Non-RFC Compliant Characters: NONE
rpc_decode arguments:
    Ports to decode RPC on: 111 32771
    alert_fragments: INACTIVE
    alert_large_fragments: ACTIVE
```

Fig. 1 Salida de SNORT



Instalación de SNORT en Windows

512MB de memoria puede manejar redes de miles de sistemas.

NIDS dentro de la red

Muy probablemente no lo colocará delante del firewall. La idea es dejar al firewall filtrar. Si lo pongo delante obtendré la mayor cantidad de paquetes pero también de ruido. También deberá estar detrás de los dispositivos que reciban a sus usuarios remotos (VPNs, conexiones wireless).
Recordemos que si el tráfico está encriptado SNORT no lo detectará. Como regla general debería colocar el NIDs tan atrás como le permitan los componentes que encriptan el tráfico pero que sea lo suficientemente lejos como para alcanzar a capturar el tráfico a través de muchos segmentos y subredes como sea posible.

¿Cómo instalo SNORT?

Snort es básicamente un sniffer de redes en modo promiscuo. En el mundo Unix se utiliza libpcaop como el driver para captura de paquetes. Loris Degioanni hizo la portación para Windows en " WinPcap".
Entonces qué es winPcap. Es un filtro de paquetes que opera a nivel del kernel, es una DLL de bajo nivel y una librería de alto nivel (independiente del sistema wpcap.dll) basada en libpcap 0.6.2. Uno se puede bajar WinPcap en http://winpcap.polito.it. Winpcap también soporta el excelente sniffer del mundo OPen Sourde: "Ethereal" (www.ethereal.com). Instalar WinPcap es muy sencillo.

CodeCraft ha sido responsable por:

- Escritura y mantenimiento del Win32 puerto de Snort1.8, 1.9, 2.0y 2.1 de Unix,
- Soporte inicial para Microsoft SQL. Servidor en el módulo loggin de la base de datos.
- Desarrollar el soporte integrado para Snort para correr como un servicio Win32.
- Desarrollar la instalación de Snort wizard paraWindows.

http://www.codecraftconsultants.com/Snort.aspx o www.snort.org

Una vez que ha hecho el download de la página de Codecraft, la instalación es más que sencilla. Deberá tomar algunas decisiones en el camino como, por ejemplo, qué base de datos utilizará: MySQL o ODBC (en este caso deje la selección por default). Pero quizá quiera hacerlo a una base SQL o Oracle. El resto son simples decisiones de ubicación de archivos, etc.
Aquel que desee usar Snort de forma profesional podrá usar la documentación en su web-page o excelentes libros dedicados a Snort. Allí aprenderá a:
-Configurarlo
-Configurar las reglas
-Setear las alertas y los logs
-Correrlo como un servicio

Pero, veamos cómo funciona Snort.

Al momento de ejecutar el .exe la siguiente información deberá ser provista: 1) dónde escribir los logs y 2) dónde encontrar el archivo de configuración.

Esta información se provee cuando lanzamos Snort desde la línea de comando:

```
Snort –l C:\snort\log –c C:\etc\snort.conf –A console
```

-A le dice que deberá mostrar la salida en la pantalla.

La figura 1 nos muestra la salida de Snort.

Si desea activar una alerta interesante, simule lo que hace el ataque de Nimda y Code Red: Desde su web.browser haga:
http://www.prueba.com.ar/cmd.exe (prueba es por supuesto genérico)

Este alerta por supuesto también quedará grabado en c:\snort.log

Se recomienda tener cuidado con el sitio web que se usa ya que muchos administradores considerarían esto como el ataque de un hacker. Otro modo de activar de forma sencilla un alerta es enviar un ping a un servidor de nuestra subred con un paquete extremadamente grande:

```
ping  -l 32767 192.168.1.22
```

Este paquete dirigido a la máquina con número IP 192.168.1.22 no es de rutina y Snort nos dará la alerta.

Más allá del primer nivel

Lo anterior fue "jugar" a ver cómo funciona Snort. Es una aplicación muy completa y es posible incrementar sus posibilidades. Recomendamos leer la bibliografía sobre Snort para volverse un experto.

¿Qué es ACID?

Normalmente Snort aparece en conjunto con las siglas ACID. Supongamos que deseamos realizar Datamining sobre los datos de alertas de Snort. Se puede incluir un Addon desarrollado por la Universidad de Carnegie Mellon que permite realizar esto.

¿Qué es un NIDS?

NIDS es básicamente un SNIFFER especializado. Un "olfateador" de paquetes. Estudia cada paquete que pasa por la interfase tratando de localizar determinadas formas precisas dentro del payload de los paquetes donde residen específicamente los códigos maliciosos.
Con un NIDS como SNORT podrá vigilar dentro de su red el contenido y la correspondencia de cada paquete que atraviesa su organización y detectar así una gran cantidad de ataques y tráfico hostil. -Todo esto en tiempo real!

Open VPNs

Autor: **Luis Otegui**

Quién es quién en el mundo de las VPNs bajo Linux

Seguramente en el último tiempo ha escuchado hablar de VPNs. Mucha gente habla de ellas como si fueran la panacea universal en la defensa de las comunicaciones de la empresa, o como si fueran estrictamente necesarias para el funcionamiento de las mismas. Es verdad que en ciertos escenarios se convierten en ayudas muy convenientes, pero es necesario detallar sus principales usos y ver qué tipo de implementación es la más adecuada a su escenario. Definimos primero una VPN o Red Privada Virtual como una implementación que permite realizar una conexión segura con alguna red segura también, pasando por un medio inseguro.

Los típicos escenarios de implementación de una Red Privada Virtual son dos. El primero consiste en usuarios que deben conectarse a una red privada corporativa mediante una conexión encriptada, a través de un medio no confiable, como Internet o una conexión Wi-Fi, en un estilo de conexión cliente-servidor.

En el segundo, dos redes privadas seguras se conectan vía un enlace punto-a-punto cifrado, con un modelo de conexión P2P (peer to peer). Lo más común para desarrollar este último tipo de conexión es la implementación de routers con soporte VPN. Cisco soporta desde su IOS varios protocolos de encriptación. Sin embargo, firewalls dedicados pueden utilizarse de la misma manera.

Los puntos flacos de las implementaciones de Redes Privadas Virtuales son dos: la performance (la encriptación puede ser una gran devoradora de recursos de sistema), y lo limitada de la utilización de estas implementaciones en conjunto con NAT (Network Address Translation). En general, las "puntas" de un enlace VPN no se colocan en LANs corporativas por este último motivo, excepto por el caso de varios clientes conectados a un VPN server, descrito más arriba. Para solucionar el problema de conjugar VPNs y NAT, muchas veces el VPN server se monta sobre el firewall de la LAN corporativa, pero esto, como se ha dicho, trae aparejados problemas de sobrecarga para el sistema. Veamos qué herramientas tenemos disponibles para crear túneles seguros en la red sobre Linux:

FreeS/WAN (ahora OpenS/WAN)

FreeS/WAN (http://www.freeswan.org/) es la implementación de un método de encriptación más longeva en el mundo Linux, aunque recientemente ha sido sustituida por su sucesora, OpenS/WAN. Se basa en IPSec, un backport de encabezados de seguridad de IPV6 a IPV4. Tiene las ventajas de ser la más robusta y poderosa de todas las implementaciones, además de ser la más aceptada. Se compone de un par de módulos y comandos en espacio de usuario, los cuales son instalados por FreeS/WAN. La línea de kernels 2.6 ya incluyen estos módulos, pero, en general, la línea 2.4 no, por lo que habrá que parchear el kernel, y recompilarlo para agregar la funcionalidad de IPSec a nuestro sistema. Lo más probable es que FreeS/WAN esté incluida en su distribución de Linux, pero como el proyecto ha caducado recientemente, le recomiendo "pasarse" a OpenS/WAN, un proyecto paralelo fundado por alguna de la gente que desarrollaba FreeS/WAN. Lo más probable es que en un futuro muy cercano las distribuciones principales de Linux reemplacen sus paquetes de FreeS/WAN por OpenS/WAN. Mientras tanto, habrá que compilarlo bajando el código de www.openswan.org/.

Las ventajas más reseñables de la implementación IPSec, sea vía FreeS/WAN o vía OpenS/WAN, son su robustez, la interoperabilidad con otros sistemas operativos, y la estabilidad del producto, dado que ya lleva varios años de desarrollo. Como puntos en contra, podemos resaltar el grado de conocimiento necesario para poder realizar una implementación exitosa, y el hecho de que, al estar diseñado para conectar redes enteras a través de túneles seguros, no "escalea" bien hacia abajo. Esto es, tiene requerimientos de sistema demasiado importantes, y puede que le quede "grande" a su escenario.

OpenSSH

Más que estándar en el mundo Linux como herramienta de shell remoto, poca gente sabe de la funcionalidad de los SSH servers como reenviadores de paquetes encriptados. Vía esta implementación, es posible crear un túnel seguro para cualquier servicio TCP que corra en un solo puerto, vía los switches –L y –R.

Es posible además hacer túneles PPP sobre SSH (lo que normalmente se realiza vía IPSec), pero esto es desastroso en términos de recursos de sistema, llevando la carga de CPU hasta las nubes. Sin embargo, su habilidad para crear túneles seguros desde un host específico corriendo un servicio específico la coloca en el hueco dejado por IPSec. Es útil para asegurar conexiones de acceso remoto y de tipo punto-a-punto, si bien, como se ha dicho, no se desenvuelve bien cuando de enlutar tráfico entre dos redes se trata.

OpenSSH está incluida en virtualmente todas las distribuciones de Linux existentes, y sus páginas de manual son bastante claras en la forma de realizar port forwarding seguro mediante esta herramienta.

STunnel

Stunnel no es más que un wrapper SSL; todo lo que hace es encriptar port forwarding, de la misma forma que OpenSSH lo hace. Además, tiene un requerimiento que muchos encon-

Encryption Tools

1 | GnuPG / PGP Protección con cifrado avanzado

GnuPG es una implementación del estándar PGP. Mientras GnuPG es un software libre, PGP puede tener un mayor costo para algunas aplicaciones.
En la lista general: #30

2 | OpenSSL La más célebre biblioteca de cifrado para SSL/TLS

Set de heramientas robusto, de nivel comercial, completo en características, y "Open Source" implementando los protocolos "Secure Sockets Layer" y "Transport Layer Security" así como una biblioteca de cifrado de propósito general potente.
En la lista general: #41

3 | Tor Un sistema anónimo de comunicación por Internet

Herramienta para personas y organizaciones que quieren mejorar su seguridad en Internet.
En la lista general: #59

4 | Stunnel Una envoltura criptográfica SSL de propósito general

Trabaja como una envoltura de cifrado SSL entre un cliente remoto y un servidor local (ejecutable por inetd) o remoto. Puede agregarle funcionalidad SSL a daemons utilizados comúnmente, y servidores de IMAP sin cambios en el código del programa.
En la lista general: #79

5 | OpenVPN Una completa solución de SSL

Solución de conectividad de open source basada en SSL VPN Virtual Private Network que ofrece conectividad punto-a-punto con validación, jerárquica de usuarios y host conectados remotamente.
En la lista general: #92

6 | TrueCrypt Disco de encriptación para Windows y Linux

TrueCrypt es un software gratuito para encriptar y ocultar en la computadora datos que el usuario considere reservados.
En la lista general: #97

trarán molesto, la necesidad de instalar certificados de seguridad, ya sea firmados por nosotros mismos, o por alguna autoridad certificadora. STunnel está incluida en todas las distribuciones importantes, y su man page es bastante clara acerca de su utilización.

OpenVPN

OpenVPN nace, según su autor, para cubrir la necesidad de un sistema de VPN más sencillo que IPSec. Basado en OpenSSL, corre en espacio de usuario, y lo que hace es encapsular el tráfico encriptado en paquetes "normales" (es decir que no es necesario modificar el kernel). Como corre en espacio de usuario, es mucho más fácil de portar de un sistema a otro y, al basarse en OpenSSL, tiene todas sus ventajas así como sus debilidades.
La única contra significativa de este producto es que sólo es capaz de realizar un túnel en un determinado puerto, es decir que si queremos realizar múltiples conexiones a un server, tendremos que arrancar en el mismo tantos otros procesos, escuchando cada cual en su puerto. La versión 2.0 promete soportar múltiples conexiones, convirtiéndola así en una buena alternativa para escenarios de acceso remoto.
El sitio del producto (http://openvpn.net/) incluye información muy detallada acerca de la instalación, configuración y mantenimiento. Hay paquetes disponibles para algunas distros, mantenidos en forma independiente.

PoPToP

Basado en el protocolo de encriptación de bajo nivel de Microsoft Point-to Point Tunneling Protocol (PPTP), esta implementación tiene sus buenos fanáticos en el mundo Linux, básicamente porque al formar parte de la suite Windows NT desde la versión 4.0, hace las cosas fáciles como solución cross-platform. Además, PPTP no sólo hace túneles IP, sino además NETBEUI e IPX. Ahora bien, así como comparte estas virtudes, también sus falencias. MSCHAP, el protocolo de encriptación utilizado por PPTP, ha mostrado ser extremadamente vulnerable. Esto ha sido parcialmente arreglado por el parche MSCHAPv2, pero para varios analistas, el protocolo simplemente no es confiable. A menos que se pueda configurar a todos los clientes y servidores para utilizar MSCHAPv2, no es recomendable instalar esta solución. Bajo Linux, PPTP se implementa como dos aplicaciones separadas, PoPToP para la parte del servidor, y PPTP Client como cliente. En www.poptop.org/ y en http://pptpclient.sourceforge.net/ se encuentra información acerca de la instalación y configuración de ambas partes de esta suite.

Conclusión

Dado lo extendida de su implementación, lo estable de su código, y su potencia, IPSec, vía FreeS/WAN u OpenS/WAN, es la implementación más recomendable para la realización de una VPN. Sin embargo, en un futuro muy cercano, OpenVPN podría plantarles una dura batalla en el mercado de los usuarios que recién se inician a las redes privadas virtuales, o que no necesitan una solución de tanta potencia para sus necesidades. Stunnel y OPenSSH ayudan de manera rápida a implementar túneles seguros a una aplicación específica (un punto-a-punto en su sentido más estricto, podríamos decir), y, si se está dispuesto a aceptar los riesgos, PoPToP es una solución rápida para conectividad cifrada entre los mundos de Linux y Windows. Espero que este breve resumen los ayude a decidir qué implementación es la más conveniente a sus necesidades, o cuando menos, les despierte la curiosidad sobre un tema que en el futuro cercano será mucho más común que hoy en día.

OS Detection Tools

1 | P0f
Herramienta de identificación de sistemas operativos
P0f puede identificar el sistema operativo de un host remoto con solo examinar los paquetes capturados aun cuando éste está detrás de un paquete de firewall. P0f no genera ningún tráfico adicional, directo o indirecto.
En la lista general: #33

2 | Xprobe2
Herramienta de identificación de sistemas
XProbe es una herramienta que sirve para determinar el sistema operativo de un host remoto. Logran esto utilizando algunas de las mismas técnicas que Nmap al igual que muchas ideas diferentes. Xprobe siempre ha enfatizado el protoclo ICMP en su enfoque de identificación.
En la lista general: #42

Packet Crafting Tools

1 | Hping2
Utilidad de observación para redes con esteroides
Hping2 ensambla y envía paquetes de ICMP, UDP o TCP hechos a medida y muestra las respuestas. Fue inspirado por el comando ping, pero ofrece mucho más control sobre lo enviado. También tiene un modo traceroute bastante útil y soporta fragmentación de IP. Esta herramienta es particularmente útil al tratar de utilizar funciones como las de traceroute/ping o analizar de otra manera, hosts detrás de un firewall que bloquea los intentos que utilizan las herramientas estándar.
En la lista general: #6

2 | Scapy
Herramienta interactiva de manipulación
Scapy permite controlar el contenido de todos los campos de los datagramas que generemos y ello unido a la versatilidad que ofrece python como lenguaje y su intérprete da como resultado un buen aliado a tener en cuenta.
En la lista general: #28

3 | Nemesis
Inyección de paquetes simplificada
El Proyecto Nemesis está diseñado para ser una pila de IP humana, portable y basada en línea de comandos para UNIX/Linux. El set está separado por protocolos, y debería permitir crear scripts útiles de flujos de paquetes inyectados desde simples scripts de shell.
En la lista general: #58

4 |Yersinia
Herramienta de múltiples protocolos para ataques de bajo nivel
Yersenia es una herramienta de ataque de bajo nivel para testeo de penetración. Es capaz de diversos ataques sobre múltiples protocolos.
En la lista general: #66

Port Scanners

1 | Superscan
El escáner de TCP para Windows de Foundstone
Un escáner de puertos de TCP, pinger y resolvedor de nombres basado en connect(). Puede manejar escaneos por ping y escaneo de puertos utilizando rangos de IP especificados. También puede conectarse a cualquier puerto abierto descubierto utilizando aplicaciones "ayudantes" especificadas por el usuario (e.g. Telnet, Explorador de Web, FTP).
En la lista general: #22

2 | Angry IP Scanner
Un rápido escáner de direcciones IP de una red local
Angry IP scanner es una pequeña herramienta que analiza y monitoriza el estado de las direcciones IP en una red local en Windows. Puede analizar cualquier IP para comprobar si responde, resolver el nombre de host e intentar conectar con aquellas que especifiques en el diálogo de configuración.
En la lista general: #51

3 | Unicornscan
Rápido escáner de puertos y protocolo
Un escáner de puertos y protocolo con gran potencia y velocidad. Un escáner que se adapta a redes muy grandes manteniendo una velocidad realmente alta. El escáner es veraz ya que dice al probador exactamente qué datos se están devolviendo en un formato claro. Los resultados pueden ir desde a una base de datos SQL para que puedan ser revisados.
En la lista general: #78

4 | Scanrand
Escáner de puertos y host
Scanrand escanea puertos y descubre host con un diseño muy similar al Unicornscan. Utiliza técnicas de criptografía para prevenir ataques y manipulaciones de los resultados del escaneo. Esta utilidad forma parte de un paquete de software llamado Paketto Keiretsu.
En la lista general: #86

Traffic Monitoring Tools

1 | Ntop
Un monitor de uso de tráfico de red
Ntop muestra el uso de la red en una manera similar a lo que hace top por los procesos. En modo interactivo, muestra el estado de la red en una terminal de usuario. En Modo Web, actúa como un servidor de Web, volcando en HTML el estado de la red. Viene con un recolector/emisor NetFlow/sFlow, una interfaz de cliente basada en HTTP para crear aplicaciones de monitoreo centradas en top, y RRD para almacenar persistentemente estadísticas de tráfico.
En la lista general: #36
Otra clasificación: packet sniffers

2 | Ngrep
Muestra y busca paquetes
Ngrep se esfuerza por proveer de la mayoría de características comunes del "grep" de GNU, aplicándolas a la capa de network. ngrep es consciente de la presencia de pcap y permite usar expresiones regulares que concuerden con el "payload" de los paquetes. Actualmente reconoce TCP, UDP, e ICMP sobre Ethernet, PPP, SLIP e interfaces nulas, y comprende la lógica de un filtro "bpf" de la misma manera que herramientas más comunes de sniffing como tcpdump y snoop.
En la lista general: #38
Otra clasificación: packet sniffers

3 | Ether Ape
Un monitor de red gráfico para Unix basado en etherman
EtherApe muestra toda la actividad de red gráfica: conexiones IRC, web, correo, etc. Soporta Etherner, FDDI, Token Ring, ISDN, PPP y SLIP.
En la lista general: #43
Otra clasificación: packet sniffers

4 | SolarWinds
Herramientas de descubrimiento/ monitoreo/ataque para redes
SolarWinds ha creado y vende docenas de herramientas de propósito especial orientadas a administradores de sistemas. Las herramientas referidas a la seguridad incluyen varios escáneos de descubrimiento para redes y un cracker por fuerza bruta de SNMP.
En la lista general: #46
Otra clasificación:password crackers

5 | Nagios
Host de código libre para monitorear equipos y servicios
Nagios es un sistema de monitorización de red. Controla los equipos y los servicios que se especifican, alertando cuando las cosas van mal y cuando están mejorando. Puede monitorear servicios de red (smtp, pop3, http, nntp, ping, etc.) y recursos del equipo.
En la lista general: #67

6 | Argus
Auditor de las transacciones de IP de red
Argus es un Monitor de tiempo real designado a rastrear y reportar el estatus y la performance de todas las transacciones vistas en la red.
En la lista general: #83

Traceroute Tools

1 | Firewalk
Avanzado traceroute
Firewalk emplea traceroute como técnica para analizar la reacción de los paquetes IP para determinar filtros ACL y mapas de red. Esta herramienta clásica fue rescrita en octubre de 2002.
En la lista general: #50

2 | Tcptraceroute
Implementación de traceroute usando paquetes de TCP
El problema es que con la expansión del uso de firewalls en el módem de Internet, muchos de los paquetes que el convencional traceroute envía, terminan siendo filtrados, haciendo que sea imposible rastrear completamente la trayectoria.
En la lista general: #90

Password Crackers

#1 | Cain and Abel **Recuperación de passwords para Windows**
Herramienta de recuperación de passwords gratuita para los sistemas operativos de Microsoft.
En la lista general: #9
Otra clasificación: packet sniffers

#2 | John the Ripper **Cracker de hashes de passwords multi-plataforma**
Programa de criptografía rápido que aplica fuerza bruta para descifrar contraseñas.
En la lista general: #10

#3 | THC Hydra **Cracker de autenticación de red paralelizado**
Esta herramienta permite realizar ataques por diccionario rápidos a sistemas de entrada por red, incluyendo telnet, ftp, http, https y más.
En la lista general: #15

#4 | Aircrack **La herramienta más rápida de crackeo de WEP/WPA**
Herramienta de crakeo para 802.11a/b/g WEP y WPA. Puede atacar redes utilizando métodos avanzados de criptografía o a través de la fuerza bruta.
En la lista general: #21
Otra clasificación: wireless tools

#5 | L0phtcrack **Aplicación de recuperación y auditoría de passwords**
L0phtCrack intenta crackear los passwords de Windows a partir de las hashes que puede obtener de máquinas con Windows NT/2000 independientes, servidores en red, controladores primarios de red o Active Directory.
En la lista general: #27

#6 | Airsnort **Herramienta de crackeo del cifrado WEP de 802.11.**
Herramienta para redes inalámbricas capaz de recuperar llaves de encriptación. Monitorea la red reuniendo una cantidad de paquetes hasta "adivinar" la clave usada en la encriptación.
En la lista general: #31
Otra clasificación: wireless tools

#7 | SolarWinds **Herramientas de descubrimiento/monitoreo/ataque para redes**
SolarWinds ha creado y vende docenas de herramientas orientadas a administradores de sistemas.
En la lista general: #46
Otra clasificación: traffic monitoring tools

#8 | Pwdrmp **Herramienta de recuperación de passwords**
Pwdump permite recuperar las hashes de passwords de Windows localmente o a través de la red aunque Syskey no esté habilitado.
En la lista general: #47

#9 | RainbowCrack **Una innovadora herramienta**
Es un cracker de hashes que precomputa todo los plaintext posibles uno por uno y los almacena en la "rainbow table". Aunque tome tiempo precomputar la tabla, puede ser más rápido que un cracker de fuerza bruta.
En la lista general: #49

#10 | Brutus **Cracker de autenticación de fuerza bruta para redes**
Este cracker sólo para Windows se lanza sobre servicios de red de sistemas remotos tratando de averiguar passwords utilizando un diccionario y permutaciones de éste.
En la lista general: #77

Herramienta para cracking de passwords en Windows.

Rainbow Crack

En este artículo detallamos la evolución de "las herramientas" para crackear los passwords de los sistemas operativos Windows. "LopthCrack " fue "indiscutida" hasta la aparición de "RainbowCrack".

Autenticación y Passwords

El proceso de presentar un usuario sus credenciales al momento del logon se denomina autenticación. Usualmente se realiza dando el userID (nombre de usuario) y password asociado. Aunque también son bastante populares otros métodos llamados en forma genérica biométricos (por huellas digitales, cara, voz, retina entre otros). Existen muchas instancias en la que uno debe autenticarse en una red. Entre otras:

I) Un logon a la red de nuestra empresa.
II) Cuando accedo remotamente a la red de la empresa (dial-up o mediante una VPN).
III) Acceso a un web-server en nuestra intranet o desde Internet.
IV) Acceso wireless a un access point.

Cada uno de ellos tiene sus métodos y protocolos de autenticación.

Las passwords de los usuarios componen uno de los riesgos más grande a la seguridad de las redes. Este riesgo incluye la creación de las passwords, el modo en que los usuarios las protegen, cómo el sistema operativo las guarda y cómo las password son transmitidas a través de la red.

El sistema operativo es el responsable de guardar y transmitir a través de la red las "credenciales" (nombre de usuario y password) para las cuentas.

Windows 2000/2003 y XP soportan una variedad de distintos protocolos para transmitir las credenciales. También existen una variedad de formas de guardar las credenciales.

Protocolos de autenticación

Los siguientes protocolos son soportados por Windows NT:

- *LAN Manager (LM)*
- *NTLM*
- *NTLMv2*

Windows 2000-2003 y XP usan

- *Kerberos v5*

como el método de autenticación por default si utilizan Active Directory (AD). Ya que es muy posible que en nuestra infrestructura tengamos clientes "legacy" (Windows 95,98 etc) NT, Windows 2000/2003 y XP también soportan las autenticaciones anteriores (LM, NTLM y NTLMv2). Hay que recordar que éstas son autenticaciones más débiles que Kerberos y por lo tanto mucho más sencillas de comprometer.

Historia de Lopht crack

Hace unos años The Lopht mostró la debilidad de la autenticación LM de Windows. Lopht introdujo su programa de crackeo de passwords. Y, se transformó en el programa más popular de password-craking del sistema operativo Windows. Lophtcrack LC5 (ver atstake INC., www.atstake.com) es una herramienta administrativa muy respetada y LM ha sido reemplazada por NTLM, NTLMv2 y Kerberos v5. Pero ha sido superado por Rainbowcrack.

Importancia de conocer LC5 y Rainbow Crack

Del uso de LC5 los administradores pudieron aprender cómo proteger aún más sus sistemas: promoviendo el uso de passwords complejos y sabiendo como proteger las cuentas importantes. Investigar y aprender cómo funciona Rainbowcrak es también una muy buena idea.

Sobre Rainbow Crack

Utilizando un método llamado Master-Time memory Trade-Off Technique (basada en trabajos anteriores de Hellman), Phillipe Oechslin propuso una metodología capaz de crackear los passwors de Windows LM 12 veces más veloz que LC5. La idea es muy simple y se basa en usar tablas pre-calculadas con los hashes de todas las combinaciones posibles de caracteres en los passwords de Windows. Esto, junto a un algoritmo de búsqueda muy eficiente logra el factor 12 antes mencionado. Su trabajo original puede verse en http://lasecwww.epfl.ch/php_code/publications/search.php?ref=Oech03.

El método fue originalmente introducido para el protocolo LM, pero hoy es posible aplicarlo a NTLMv2 que permite utilizar el



conjunto de caracteres Unicode (con mayúsculas y minúsculas) y usar hasta 128 caracteres (LM permitía solo 14 y mayúsculas). El algoritmo se lo llama "Rainbow Crack".

Factor 12 Rainbow Crack

El factor tiempo ha sido siempre considerado el más importante en password-cracking: si los passwords son suficientemente complejos, lleva mucho tiempo poder crackearlas y las hace seguras. Hoy máquinas mucho más poderosas, máquinas que pueden actuar en conjunto y ahora RainbowCrack contribuyen a reducir los tiempos de crackeo.

Sin embargo existen una serie de acciones que podemos hacer para proteger nuestros sistemas de password cracking.

1. Utilizar protocolos de autenticación fuertes

Kerberos es el protocolo de autenticación de member servers o workstations en dominios con Windows 2000/2003/XP. En caso que tengamos sistemas "legacy" habrá que configurar que sea NTLMv2 (y no LM o NTLM) el protocolo de acceso. Esto puede hacerse

- Con group policies (en dominios Windows 2000/2003).
- En Windows NT SP4, modificando el Registry.
- En Windows 95/98, instalando "Active Directory" client y modificando el Registry.

Es importante eliminar el almacenamiento de los hashes LM en la base de datos de las passwords. Esto está por default en Windows 2003. Se debe modificar el Registry para sistemas operativos anteriores.

2. Utilizar protocolos de acceso remoto fuertes

Usuarios en su casa o empleados fuera de las oficinas accederán remotamente a nuestra red. En muchos casos es importante imponer autenticación. El acceso remoto puede ser vía dial-up (telefónico o VPN), WEB o wireless.

Existen en Windows un número muy grande de metodologías de autenticación cuando se accede remotamente: incluyendo anonymous, basic (passwords en texto plano), integrated (variantes de LM o Kerberos), PAP, CHAP, MS-CHAP, MS-CHAPv2 and EAP (y variantes como PEAP y smart cards).

Los seteos por default (por defecto) son en general bastante débiles y es preciso llevarlos a lo máximo posible. Recordemos que encima de los problemas de autenticación en nuestra red aquí estamos realizando la comunicación en redes no confiables.

En los entornos de Windows 2000/2003 es posible definir además políticas de acceso remoto (Remote access policies) que permite la configuración de opciones para la autenticación en el acceso remoto mucho más granular.

3. Utilizar comunicaciones seguras

Si las credenciales viajan debemos proteger las comunicaciones. Estos métodos incluyen:

VPNs
SSL
IPsec
SMB signing

4. Proteger las bases de datos de las passwords

Todo sistema operativo por razones de seguridad contendrá uno o más archivos con una base de datos con la información de los usuarios. Esta base de datos alojará toda la información del usuario, incluyendo su password. Por supuesto que esos archivos contendrán la información, al menos los passwords, encriptados de modo de impedir su conocimiento en caso de ser comprometido el archivo. Por eso, resulta imperativo proteger esos archivos.

En Widows NT esa información se guardaba en la SAM (Security Accounts Manager) database. Hoy toda la familia de SOs Windows para workstations incluyendo Windows 2000 Professional y XP también contienen y usan una SAM. Por default Windows 2003 Server también contiene y usa una SAM. Pero cuando organizamos nuestra infraestructura en dominios, con Active Directory (AD), los llamados "Domain Controlers" (DC) contendrán la base de datos centralizada debidamente protegida en el archivo NTDS.DIT. Es por esto que debe tener en cuenta los siguientes consejos:

- Proteja los backups: los backups contienen copias de la SAM o ntds.dit
- Proteja físicamente las computadoras: si el sistema puede accederse físicamente, un atacante puede ser capaz de rebootearla en otro sistema operativo.
- Las cuentas de administrador deben ser limitadas, muy bien asignadas y auditadas: existen herramientas administrativas como ERD Commander y variantes de pwdump que en manos de un atacante con privilegios de administrador permiten crackear las passwords del sistema.

5. Investigar las técnicas de password cracking

Un programa de password cracking será una excelente inversión para el grupo de seguridad de la empresa. Conocer las herramientas que un posible intruso usará nos preparará para la defensa. Tendremos noción de las posibles metodologías y más importante aún de los tiempos que puede llevar realizar un cracking de passwords en nuestros sistemas.

LC5 de atstake Inc. ha sido desde hace años la herramienta para permitirnos entender y realizar auditorias de passwords. LC5, también utiliza tablas de RainbowCrack. Si uno desea testear las tablas de RainbowCrack directamente, existen gran número de websites con información detallada.

6. Forzar políticas de passwords y realizar entrenamientos de concientización y auditorías de passwords

Implemente políticas de passwords. Por ejemplo si utiliza passwords con más de 15 caracteres automáticamente requerirá el uso del protocolo de autenticación NTLM. Recordar que cuanto más larga es la password más difícil será crackearla. No solo el largo del password es importante sino la utilización de caracteres menos comunes dificultarán el crackeado.

Para proteger nuestros sistemas no basta con implementar políticas y tecnologías. Es fundamental promover entrenamiento de concientización a nivel de los usuarios. Es difícil pretender que el usuario entienda la importancia de seguir políticas de passwords. La concientización reducirá por tanto el esfuerzo requerido para lograr la aplicación de políticas.

Se deben realizar esfuerzos de enseñar como crear passwords complejas y demostraciones de cómo se pueden crackear password. Cuando la gente toma conciencia de cuán fácilmente se pueden crackear password muy sencillas los mentaliza al uso de passwords más complejas. También es posible entrenar cómo impedir social engineering.

Packet Sniffers

1 | Wireshark

Oliendo el pegamento que mantiene a Internet unida

Wireshark (conocido como Ethereal) es un analizador de protocolos de red para Unix y Windows. Nos permite examinar datos de una red viva o de un archivo de captura en algún disco. Se puede examinar interactivamente la información capturada, viendo información de detalles y sumarios por cada paquete. Wireshark tiene varias características poderosas, incluyendo un completo lenguaje para filtrar lo que queramos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

En la lista general: #2

2 | Kismet

Un poderoso sniffer para redes inalámbricas

Kismet es un poderoso sniffer para redes inalámbricas. Es un sniffer de red sobre el protocolo 802.11b, a y g. También es lo que se denomina un analizador de redes (network disector). Es capaz de realizar sniffing sobre la mayoría de las tarjetas inalámbricas, detección automática de bloques de IP vía paquetes UDP, ARP y DHCP, lista de equipos Cisco vía Cisco Discovery Protocol, loggin de paquetes bajo criptografía débil y con archivos de paquetes compatibles con Ethereal y tcpdump. También incluye la habilidad de graficar las redes detectadas y los rangos de redes estimados en mapas ya bajados o archivos de imágenes provistos por el usuario. El soporte para correr bajo el sistema operativo Windows está aún en desarrollo preliminar, así que en este caso Netstumbler es la opción. Usuarios Linux (y aquellos con PDAs bajo Linux) puede querer mirar al scanner Wellenreiter.

En la lista general: #7
Otra Clasificación: wireless tools

3 | Tcpdump

Sniffer clásico para monitorear la redes y adquirir datos

Es un analizador de paquetes de red (sniffer) muy conocido y apreciado. Puede ser usado para printear los headers (encabezamientos) de los paquetes en una interface de red que coincidan con una dada expresión. Se puede usar esta herramienta para hallar problemas de redes y para monitorear las actividades de las mismas. Hay una portación lamada WinDump para Windows. Tcpdump es también la fuente del Libcap/WinPcap, la librería de captura de paquetes usada por Nmap. Pero muchos usuarios prefieren el sniffer Ethereal que es más nuevo.

En la lista general: #8

4 | Cain and Abel

Recuperación de passwords para Windows

Cain & Abel es una herramienta de recuperación de passwords gratuita para los sistems operativos de Microsoft. Permite una fácil recuperación de varias clases de password.

En la lista general: #9
Otra Clasificación: password crackers

5 | Ettercap

Por si acaso todavía pensemos que usar switches en las LANs nos da mucha seguridad extra

Ettercap es un interceptor/sniffer/registrador para LANs con ethernet basado en terminales. Soporta disecciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También es posible la inyección de datos en una conexión establecida y filtrado al vuelo y aun manteniendo la conexión sincronizada. Muchos modos de sniffing fueron implementados para darnos un set poderoso y completo de sniffing. También soporta plugins. Tiene la habilidad para comprobar si estamos en una LAN con switches o no, y de identificar huellas de sistemas operativos para dejarnos conocer la geometría de la LAN.

En la lista general: #11

6 | Dsniff

Un juego de poderosas herramientas de auditoría y pruebas de penetración de redes

Grupo de herramientas poderosas para auditar redes y realizar test de penetración. Incluye varias herramientas: dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, y webspy monitorean pasivamente una red en busca de datos interesantes (passwords, e-mail, archivos, etc.). arpspoof, dnsspoof, y macof facilitan la intercepción de tráfico en la red normalmente no disponible para un atacante. sshmitm y webmitm implementan ataques activos del tipo monkey-in-the-middle hacia sesiones redirigidas de SSH y HTTPS abusando de relaciones débiles en sistemas con una infraestructura de llaves públicas (PKI) improvisados.

En la lista general: #17

7 | NetStumbler

Sniffer gratuito de 802.11 para Windows

Netstumbler se define como un sniffer de redes wireless no intensivo pues identifica a los access points que están realizando broadcast de sus nombres (SSID), además permite identificar la dirección MAC del dispositivo. Trabaja sobre plataforma PC Windows.

En la lista general: #18
Otra Clasificación: wireless tools

8 | Ntop

Un monitor de uso de tráfico de red

Ntop muestra el uso de la red en una manera similar a lo que hace top por los procesos. En modo interactivo, muestra el estado de la red en una terminal de usuario. En Modo Web, actúa como un servidor de Web, volcando en HTML el estado de la red. Viene con un recolector/emisor NetFlow/sFlow, una interfaz de cliente basada en HTTP para crear aplicaciones de monitoreo centradas en top, y RRD para almacenar persistentemente estadísticas de tráfico.

En la lista general: #36
Otra Clasificación: traffic monitoring tools

9 | Ngrep

Muestra y busca paquetes

Ngrep se esfuerza por proveer de la mayoría de características comunes del "grep" de GNU, aplicándolas a la capa de network. ngrep es consciente de la presencia de pcap y permite usar expresiones regulares que concuerden con el "payload" de los paquetes. Actualmente reconoce TCP, UDP, e ICMP sobre Ethernet, PPP, SLIP e interfaces nulas, y comprende la lógica de un filtro "bpf" de la misma manera que herramientas más comunes de sniffing como tcpdump y snoop.

En la lista general: #38
Otra Clasificación: traffic monitoring tools

10 | EtherApe

Un monitor de red gráfico para Unix basado en etherman

EtherApe muestra toda la actividad de red gráfica: conexiones IRC, web, correo, etc. Soporta Etherner, FDDI, Token Ring, ISDN, PPP y SLIP.

En la lista general: #43
Otra Clasificación: traffic monitoring tools

11 | KisMAC

Stumbler inalámbrico para Mac OS X

Este popular stumbler para el sistema operativo de Mac ofrece mucha de las aplicaciones de Kismet pero a través de una base de códigos enteramente diferente.

En la lista general: #55
Otra Clasificación: wireless tools

Security-Oriented Operating Systems

1 | BackTrak

Testea la penetración en Linux

BackTrack es una distribución Live de Linux diseñada para trabajar con la seguridad informática, en específico en lo referente a redes inalámbricas. Deriva de WHAX, que a su vez deriva de WHOPPIX.

En la lista general: #32

2 | Knoppix

Sistema general booteable desde CD o DVD

Knoppix es una distribución de GNU/Linux basada en Debian y utilizando KDE. Está desarrollada por el consultor de GNU/Linux Klaus Knopper.

En la lista general: #60

3 | OpenBSD

El sistema operativo preventivamente seguro

OpenBSD es uno de los pocos sistemas operativos que ponen a la seguridad como su prioridad. Su mayor logro fue la creación de OpenSSH.

En la lista general: #65

4 | Helix

Distribución de Linux con mentalidad de computación forense

Helix es una distribución del Knoppix Live Linux CD. Helix fue diseñado cuidadosamente para no tocar el host de la computadora.

En la lista general: #94

5 | Bastille

Un script de fortalecimiento de seguridad para Linux, Max Os X, y HP-UX

Cierra un sistema operativo, configurando proactivamente el sistema para aumentar la seguridad y disminuir su susceptibilidad. Bastille soporta Red Hat, SUSE, Debian, Gentop y distribuciones Mandrake.

En la lista general: #95

Disassemblers

1 | IDA Pro

Desensamblador de Windows o Linux

Es un desensamblador comercial usado la mayoría de las veces para ingeniería reversa. Soporta varios formatos para diferentes procesos y sistemas operativos. Este interactivo, programable, extensible y multi procesador desensamblador ahora soporta Linux así como también Windows.

En la lista general: #45

2 | OllyDbg

Debugger de Windows

OllyDbg es un debugger para aplicaciones de win32. Este debugger puede mientras el programa a depurar está ejecutándose, modificar datos de la memoria del propio proceso del programa. OllyDbg se puede bajar de forma gratuita pero no proveen de los códigos.

En la lista general: #93





a las amenazas conocidas y desconocidas



Panda
GateDefenderPerforma

Protección "conectar y olvidar" contra virus, spam y contenidos no deseados

Dispositivo SCM (Secure Content Management) escalable, de fácil manejo "conectar y olvidar", capaz de neutralizar todos los virus, spam, y contenidos web no deseados antes de que entren en su red.



Panda
GateDefenderIntegra

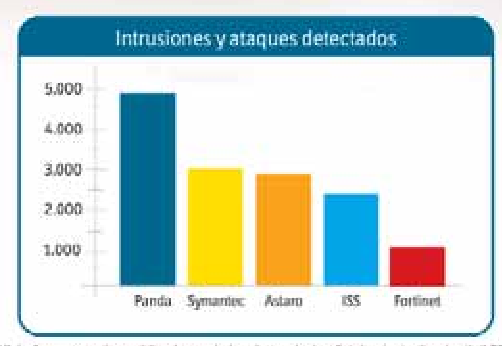
Prevención perimetral centralizada contra todo tipo de amenazas procedentes de Internet

Dispositivo UTM (Unified Threat Management) "todo en uno" de última generación, que integra firewall, Sistema de Prevención contra Intrusiones, VPN, antimalware, antispam y tecnologías de filtrado de contenidos web.

"Mejor Software 2006"
CeBIT Highlights

Mayor protección a través de la prevención

La familia GateDefender de soluciones para redes, ofrece protección perimetral proactiva constantemente actualizada contra la nueva generación de ataques informáticos, intrusiones de hackers, virus y demás malware, gracias a la combinación de avanzadas técnicas de detección on Line de amenazas conocidas y desconocidas. Incorpore las premiadas tecnologías de Panda Software y detenga todas las amenazas antes de que entren en su Red.



*N° de firmas y reglas publicados en hojas de producto oficiales (actualizado abril 2006)

Consulte su **P**anda **B**usiness **P**artner Certificado
o comuniquese al 5238 1408

Panda Software
www.panda-argentina.com.ar
info@panda-argentina.com.ar



Netcat

Es muy acertado denominar de tal manera a Netcat, dada la amplia cantidad de tareas que permite que sean hechas. Netcat es una de las herramientas más popular utilizada en el mundo, pues con ella puede reemplazarse a una suite de herramientas.

Autor: **Leonel Becchio**

Netcat es un cliente telnet, básicamente su función primordial es la lecto-escritura de datos a través de conexiones TCP o UDP. Por tal motivo, como puede ser especificado el puerto de trabajo, Netcat puede ser usado como scanner de puertos, redirector de puertos, puerta de acceso trasero (backdoor) y otras tantas cosas. Tal vez no sea la mejor herramienta o la más cómoda para trabajar, pero esta utilidad brinda lo necesario para suplir los requerimientos de una completa tarea de hacking por sí sola. La ventaja es que Netcat puede trabajar como cliente y servidor. Debemos aclarar que como todo cliente telnet, cada cosa que tipeemos, primero viaja hacia la consola remota y si es que existe un puerto a la escucha, vuelve y es mostrada en la consola local. Por tal motivo deberemos colocar dos consolas corriendo Netcat, una local y una funcionará como remota.

Netcat proviene de la época de los sistemas operativos Unix, de hecho fue lanzado primeramente para aquellos sistemas y posteriormente apareció la versión para el entorno Windows NT. Su nombre es una derivación del comando Unix cat que se utiliza para concatenar archivos. Asimismo Netcat se utiliza para concatenar sockets TCP y UDP.

La utilidad fue desarrollada para ser trabajada desde una consola por línea de comandos invocando el comando nc. Sería demasiado extenso mencionar todos los parámetros disponibles para usar con Netcat, por tal motivo veremos los más utilizados en algunos de los casos que describiremos.

Port Scanning

nc -v -w2 -z dir_IP_destino 1-200

En este caso Netcat tratará de conectarse a cada puerto entre el puerto 1 y el 200 de la dirección IP que especifiquemos. Probablemente informe sobre aquellos servicios que se encuentren corriendo en puertos comprendidos entre dichos límites. La opción -v (verbose) brinda información detallada cuando la aplicación arroja el resultado. La opción -w (wait) permite esperar una cantidad de tiempo determinada (en segundos) para que se genere la conexión TCP. La opción -z, por su parte, previene que sea enviada información adicional a una conexión TCP mientras está bajo prueba, se puede insertar una demora de tiempo entre cada prueba de puertos con el agregado de -i. El uso de -z es útil como escaneo rápido para ver qué puertos responden.

Transferencia de archivos con Netcat

Esto mismo podría ser realizado con alguna herramienta que trabaje el protocolo TFTP, pero lo haremos con Netcat. Recordando que Netcat es un cliente/servidor telnet, debemos abrir dos consolas: una funcionará como consola remota y será nuestro servidor, la otra funcionará como consola local y será nuestro cliente tratándose de conectarse al servidor.

En la consola remota escribiremos:

nc -l -p 6000 > prueba.txt

Aquí lo que hacemos es poner el puerto 6000 a la escucha y prepararlo para aceptar por él el archivo prueba.txt. El comando -l (listen) pone a la escucha el puerto especificado con -p (port).

Es importante aclarar que así como el protocolo TFTP no posee una instancia de autenticación (uno de los motivos que lo diferencian de su par FTP), con Netcat obligamos a transferir el archivo especificado por la fuerza. Esto trae como consecuencia que sea una herramienta apta para utilizarse junto a una puerta trasera de acceso (backdoor) dado que una vez encontrada la forma de mantener dicho orificio, será muy fácil transferir datos en ambos sentidos.

En la consola local escribiremos:

nc dir_IP_consola_remota 6000 < prueba.txt

Aquí lo que hacemos es indicarle a nuestro cliente que se conecte a la dirección IP en cuestión y que envíe el archivo prueba.txt dirigido al puerto 6000.

Nota: Puede parecer confuso el uso de los direccionadores < >, pero su uso se entiende de la siguiente manera. El contenido del archivo situado a la derecha del comando se direcciona (<) al puerto 6000 bajo la correspondiente IP del lado del cliente. Por su parte, del lado del servidor se vuelca el contenido que viene por el puerto 6000 al archivo .txt en cuestión (>) situado a la derecha. De esta forma, el archivo viaja desde el cliente hacia el servidor y no al revés como puede pensarse.

Lo que se suele hacer con este par de comandos es transferir datos desde y hacia un servidor que está siendo atacado. En primera instancia se genera la puerta de acceso trasera para poder entrar libremente cuando se lo requiera, posteriormente se envía por única vez una copia de la herramienta netcat al servidor atacado. Finalmente desde la máquina del intruso se manipula remotamente la utilidad enviando y recibiendo datos a placer.

Netcat como backdoor

Como última aplicación citamos el uso de netcat una vez que se encuentra en el servidor comprometido, es decir una vez encontrado el agujero por donde ingresar una y otra vez.

Una vez que hayamos subido una copia de netcat al servidor atacado, seguramente será nuestro deseo poder contar con dicha utilidad cuando la necesitemos. La idea es que netcat pueda escuchar un puerto específico y pueda conectarse remotamente desde nuestra máquina atacante.

Con el comando nc -L -p 10001 -d -e cmd.exe. La opción -L (mayúscula) le indica a netcat que no se cierre, que espere por más conexiones activándose cuando nos conectemos al puerto especificado por la opción -p. La opción -d (detach) le indica a netcat que se separe del proceso que queremos que corra. Posteriormente la opción -e (execute) le indica que ejecute el programa especificado a continuación, o sea la consola de comandos cmd.exe.

Netcats

1 | Netcat

La navaja del ejército suizo

Herramienta UNIX que lee y escribe datos a través de las conexiones de red, usando protocolos TCP o UDP. Se diseñó para ser una herramienta back-end que puede ser usada directamente o transportada por otros programas y scripts.

En la lista general: #4

2 | Socat

Transferencia de información bidireccional

Con una utilidad parecida a Netcat trabaja sobre un gran número de protocolos y a través de archivos, devices, sockets, etc. Permite conectar muchos tipos de abstracciones de entrada y salida distintas.

En la lista general: #71

Firewalls

1 | Netfilter
El firewall de paquetes del kernel Linux actual
Poderoso filtro de paquetes el cual es implementado en el kernel Linux estándar. La herramienta iptables es utilizada para la configuración.
En la lista general: #23

2 | Openbsd PF
El filtro de paquetes innovador de OpenBSD
PF (Packet Filter) es el sistema de OpenBSD para filtrar el tráfico TCP/IP y llevar a cabo la Traducción de Direcciones de Red (NAT, Network Address Translation).
En la lista general: #57

3 | IP filter
Filtro de paquetes de UNIX
Paquete de software que puede ser usado para proveer Traducciones de Direcciones de Red.
En la lista general: #87

Vulnerability Scanners

1 | Nessus
Herramienta más importante de testeo de vulnerabilidades
Es un scanner de seguridad remoto para Linux, BSD, Solaris y otros Unix. Está basado en plug-ins, tiene una interface GTK y lleva a cabo 1200 chequeos de seguridad remotos. Permite que los reportes sean generados en HTLM, XML, LaTex y texto ASCII y sugiere soluciones para problemas de seguridad.
En la lista general: #1

2 | GFI LANguard
Un escáner de red comercial para Windows
Escanea redes y reporta información como el nivel de "service pack" de cada máquina, faltas de parches de seguridad, recursos compartidos, puertos abiertos, servicios/aplicaciones activas en la computadora, datos del registro, passwords débiles, usuarios y grupos; y más.
En la lista general: #20

3 | Retina
Escáner comercial para la evaluación de vulnerabilidades hecho por eEye
Al igual que Nessus y ISS Internet Scanner, la función de Retina es escanear todos los hosts en una red y reportar cualquier vulnerabilidad encontrada.
En la lista general: #25

4 | Core Impact
Herramienta de testeo de penetración automática
Core Impact no es barato pero es considerado una de las más poderosas herramientas de explotación disponibles. Si Core Impact le resulta muy caro, puede optar por Canvas que es más barato, o por el libre Metasploit Framework.
En la lista general: #44
Otra Clasificación: vulnerability exploitation tools

5 | ISS Internet Scanner
Evaluación de vulnerabilidades a nivel de Aplicación
Comenzó en el '92 como un pequeño escáner "Open Source" escrito por Christopher Klaus. ISS creció hasta ser una enorme empresa con una amplia gama de productos de seguridad.
En la lista general: #61

6 | X-scan
Escanea vulnerabilidades de red
Es el primer analizador de vulnerabilidades totalmente gratuito que puede analizar una PC o una red completa.
En la lista general: #69

7 | Sara
Asistente de Investigación para el Auditor de Seguridad
SARA es una herramienta de evaluación de vulnerabilidades derivada del infame escáner SATAN. Tratan de publicar actualizaciones dos veces al mes y de fomentar cualquier otro software creado por la comunidad de código abierto (como Nmap y Samba).
En la lista general: #72

8 | QualysGuard
Escáner de vulnerabilidad basado en la web
QualysGuard explora las redes buscando vulnerabilidades de seguridad a los intervalos y horas especificadas por el usuario. QualysGuard se adapta a la configuración precisa de la red del cliente y se ajusta al ancho de banda disponible.
En la lista general: #73

9 | SAINT
Herramienta de red integrada para el Administrador de Seguridad
Saint es otra herramienta comercial de evaluación de seguridad (al igual que ISS Internet Scanner o Retina de eEye). SAINT corre exclusivamente sobre UNIX y solía ser gratuito y "open source" pero ahora es un producto no-libre.
En la lista general: #91

10 | MBSA
Microsoft Baseline Security Analyzer
Verifica la configuración de seguridad, detectando los posibles problemas de seguridad en el sistema operativo y los diversos componentes instalados. Es una herramienta fácil de usar diseñada por profesionales IT.
En la lista general: #100

Web Vulnerability Scanners

1 | Nikto
Un escáner de web de mayor amplitud
Escáner open source de servidores de web que busca más de 3200 archivos/CGIs potencialmente peligrosos y problemas en más de 230 servidores.
En la lista general: #12

2 | Paros proxy
Aplicación web de vulnerabilidades de proxy
Paros proxy es un proxy web que calcula las vulnerabilidades de las aplicaciones web.
En la lista general: #16

3 | WebScarab
Framework que analiza aplicaciones usando los protocolos HTTP y HTTPS
Graba las conversaciones (pedidos y respuestas) que observa y le da permiso al operador para revisarlas de varias formas. Esta herramienta está diseñada para que cualquiera que necesite ver el trabajo de una aplicación HTTP(S) pueda hacerlo.
En la lista general: #35

4 | WebInspect
Poderoso escáner de aplicaciones web
Ayuda a identificar las vulnerabilidades, tanto conocidas como desconocidas. También puede ayudar a chequear si un servidor de Internet está configurado correctamente y de esta forma prevenir ataques comunes.
En la lista general: #40

5 | Whisker/libwhisker
El escáner y la biblioteca de vulnerabilidades de CGI de Rain.Forest.Puppy
Es un escáner que nos permite poner a prueba servidores de HTTP con respecto a varios agujeros de seguridad conocidos, particularmente, la presencia de peligrosos scripts/programas que utilicen CGI. Whisker es un escáner que usa libwhisker pero actualmente está despreciada a favor de Nikito, que también usa libwhisker.
En la lista general: #70

6 | Burpsuite
Plataforma integrada para el ataque de aplicaciones web
Burp permite que un atacante combine, manual y automáticamente, técnicas para enumerar, analizar y atacar aplicaciones web.
En la lista general: #76

7 | Wikto
Scanner de vulnerabilidades web
Wikto es una herramienta que busca defectos en los webservers. Provee mucha de las mismas funcionalidades que Nikto pero le agrega algunas interesantes, como el miner Back-End y una mayor integración con Google.
En la lista general: #84

8 | Acunetix Web Vulnerability Scanner
Escáner comercial de vulnerabilidades web
Herramienta que permite escanear un sitio Web en busca de fallas de seguridad y cualquier característica del servidor que pueda llegar a poner en peligro la integridad de la página.
En la lista general: #96

9 | Watchfire AppScan
Escáner comercial de vulnerabilidades web
AppScan provee seguridad mediante el testeo de aplicaciones web, en busca de vulnerabilidades comunes.
En la lista general: #98

10 | N-Stealth
Escáner de Servidores de Web
Escáner de seguridad de servidores de web no-libre. Se actualiza más frecuentemente que los escáners de web libres como Whisker/libwhisker y Nikto. N-stealth es sólo para Windows y no se incluye el código fuente.
En la lista general: #99





RSA Laboratories

RSA Laboratories es la división de Seguridad de EMC Corporation cuya sede central se encuentra en Bedford, Massachusetts y con oficinas en Irlanda, el Reino Unido, Singapore y Japón.

El nombre de RSA proviene de las iniciales de sus fundadores: Ron Rivest, Adi Shamir y Len Adleman, quienes además, fueron los inventores de la encriptación de llave pública. A través de sus programas de investigación, desarrollo y actividades educacionales, RSA provee seguridad basada en alta tecnología. Continuamente están en la búsqueda de nuevos métodos para incluir un nuevo paradigma de autenticación y para mejorar las técnicas existentes. Particularmente, están interesados en métodos que incluyan "el aspecto humano" de autenticación, incluyendo protocolos que usen preguntas de la vida o permitir que los usuarios respondan por otros.

Historia

- En 1995 se funda Digital Certificates International, más conocida como VeriSign.
- La compañía, llamada luego Security Dinamics, adquiere RSA Data Security en julio de 1996 y DynaSoft AB en 1997.
- En febrero de 2001, compra Xcert International, Inc., una compañía privada que desarrollaba y entregaba certificados digitales basados en productos de seguridad y transacciones de e-business.
- En mayo de 2001 adquieren 3-G Internacional, Inc., compañía dedicada al desarrollo de autos inteligentes y productos de autenticación biométrica.
- En agosto de 2001 compran Securant Technologies, Inc., compañía que produce Clear Trust, n producto de identidad corporativa.
- En diciembre de 2005 adquieren Cyota, una compañía especializada en seguridad online y soluciones contra el fraude para instituciones financieras.
- En abril de 2006 compran PassMark Security.
- El 29 de junio de 2006 se anuncia que EMC Corporation compró RSA Security por 2.1 billones de dólares.

Foundstone
A Division of McAfee

Imposible no conocer FOUNDSTONE

Las empresas de cierta envergadura realizan adquisiciones de otras empresas. Se dice "dime a quién ha adquirido y te diré quién es".

Foundstone Inc. es una de las empresas de seguridad informática de mayor prestigio fundada en 1999. Ofrece una combinación de software, servicios de consultoría y dispositivos para ayudar a que las empresas estén protegidas frente a las amenazas y las vulnerabilidades.

Mc Affee en el 2003 adquirió Foundstone que hoy forma parte de ella. Invitamos a conocer Foundstone y la gran cantidad de white papers y herramientas gratuitas que ofrecen al profesional de seguridad informática. Como ejemplo podrán ver en este artículo la herramienta "Hackme Bank" y algunos de los libros cuyos autores trabajan en Foundstone. Seguramente todos reconocerán "Hacking Exposed". Stuart McClure es su co-autor y co-fundador de Foundstone.

HACKME BANK v2.0

Hackme Bank™ está diseñado para enseñar a los desarrolladores de aplicaciones, programadores y profesionales de la seguridad cómo crear software seguro. Hackme Bank es una aplicación bancaria online similar a la que se encuentra en el "mundo real" y basada en web services. Ésta fue construida con un número de vulnerabilidades conocidas y comunes. Esto les permite a los usuarios realizar exploits verdaderos contra una aplicación web y por tanto aprender temas específicos y cómo mejor arreglarlos. Los web services expuestos en Hackme Bank son usados por otras aplicaciones ofrecidas por Foundstone en "Free Tools" incluyendo "Hackme Book" y "Hackme Travel.

SANS Institute



El SANS Institute (SysAdmin, Audit, Network, Security) se estableció en 1989 como una organización dedicada a la investigación y a la educación. Provee de programas de capacitación en seguridad computacional, certificaciones profesionales y sus programas ya cuentan con más de 165 mil profesionales de la seguridad de agencias gubernamentales, empresas y universidades registrados en todo el mundo.

El SANS Institute junto con el FBI y el NIPC presentan las 20 vulnerabilidades de seguridad más críticas de Internet, que reúne las herramientas más utilizadas por los hackers.

El SANS Institute hace hincapié en la comunidad de la seguridad como un todo y por esto pone especial énfasis en reinvertir en la comunidad lo aprendido, a través de proyectos de consenso como la certificación GIAC, los trabajos prácticos de los estudiantes y la Sala de Lectura de Seguridad.

Los Instructores del SANS Institute han contribuido con varios libros de seguridad:

- Hackers Beware: The Ultimate Guide to Network Security
- Hiding in Plain Sight : Steganography and the Art of Covert Communication
- Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems
- Malware: Fighting Malicious Code
- Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses (2nd Edition)
- Network Intrusion Detection
- Network Intrusion Detection: An Analyst's Handbook

IMANAGING

intel Core™ 2 Duo inside™

Dual-core.
Haga más.

Yo, Banghó

Empresario Hiperconectado

Porque **Banghó** comprende la idiosincrasia local y aporta soluciones concretas para problemas reales. Porque su innovadora arquitectura tecnológica permite a las empresas enfrentar con éxito **operaciones de misión crítica**. Porque sus líneas de **PCs**, **servidores** y **notebooks** están certificadas bajo normas de calidad internacionales, brindando mayor poder de procesamiento, almacenamiento, seguridad y conectividad.

Por todo esto, **cada vez más argentinos eligen productos Banghó**.

BanghóPro con Procesador Intel® Core™ 2 Duo



www.**bangho**.com.ar - 0810-666-BANGHO (2264)

La Marca Nacional de Tecnología Informática

Microsoft Internet Security and Acceleration Server 2006

Tenemos entre nosotros una nueva versión del Firewall de Microsoft. En esta ocasión solo destacaremos las nuevas características, y no todas, ya que esta versión esta basada en su antecesor ISA Server 2004 al que se le agregaron nuevas y mejoradas funcionalidades.

Autor: **Cristian L. Ruiz**
MCSA, MCSE, MCT

Al observar la interfase gráfica de administración (figura 1) uno podría pensar que se trata de ISA Server 2004, pero al comenzar a configurarlo nos daremos cuenta que contamos con funcionalidades diferentes que destacan a esta versión. Para la instalación del producto tengamos en cuenta los siguientes requerimientos del sistema: CPU: Pentium III de 733Mhz o superior; Sistema Operativo: Windows Server 2003 SP1 o Windows Server 2003 R2; Memoria: 512MB de RAM o más es recomendable; Espacio en disco: 150MB de espacio disponible en una partición NTFS y más para el cache de contenido; Interfase de red: 1 para la red interna y adicionales por cada red adicional conectada.

Antes de repasar las nuevas y mejoradas características vamos a mencionar algunos detalles. Ya no esta presente como parte de la instalación la carpeta compartida que contiene el cliente de Firewall, estando disponible desde el CD de instalación para ser copiado a

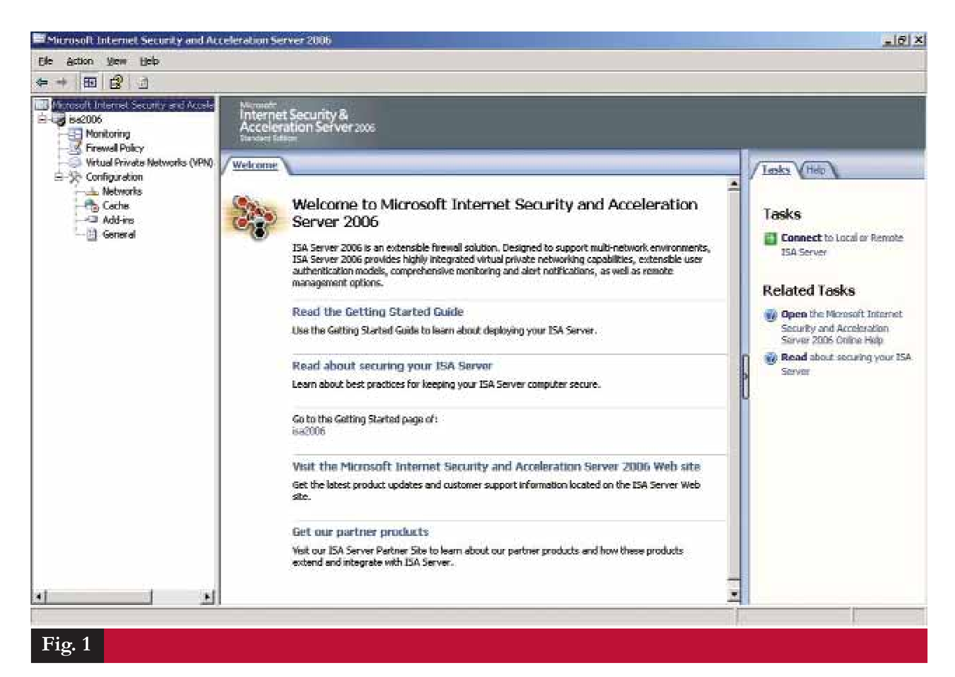


Fig. 1


Microsoft
Tu potencial. Nuestra pasión.
ENTER

Microsoft Internet Security and Acceleration Server 2006

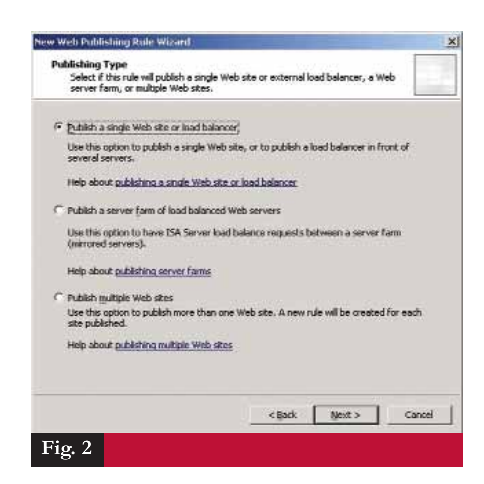


Fig. 2

cualquier carpeta compartida de una computadora de la red interna. Tampoco esta disponible el servicio Message Screener que se podía implementar usando el mismo instalador, pero en este caso el ISA Server aún sigue contando con el filtro de SMTP.

Nuevas características

A continuación nombraremos las características principales que fueron incorporadas.

1) *Customer Feedback:* lo primero que veremos es que en la consola de administración ISA Server Management, en la parte superior, existe un vínculo para configurar la opción del programa Customer Feedback. Aceptando participar de dicho programa se recolectará información anónima del sistema, que será enviada a Microsoft para que puedan hacer seguimientos de usos del producto. Obviamente, podemos optar por no aceptar dicha participación.

2) *Web publishing load balancing:* ahora se podrá publicar un conjunto de servidores Web que pertenezcan a la misma granja de servidores (se agrega el concepto de creación de granja). Se podrá publicar un sitio Web mantenido por varios servidores miembros de una granja (figura 2) donde las peticiones de los usuarios serán re-direccionadas entre estos servidores, obteniendo así balanceo de cargas y al mismo tiempo tolerancia a fallos. De esta manera ya no es necesario implementar un cluster de balanceo de cargas por separado, sino que esto lo podemos implementar por una función desde el mismo ISA Server.

3) *Single sign-on:* permite publicar varios sitios Web evitando a los usuarios presentar sus credenciales múltiples veces. Se podrá navegar entre los diferentes sitios publicados con las mismas credenciales presentadas al acceder al primer sitio. Esta funcionalidad solo se aplicará en los sitios publicados que utilicen el mismo Web Listener y que compartan el mismo nombre de dominio, como por ejemplo, ventas.microsoft.com y soporte.microsoft.com.

4) *LDAP Autenthication:* en ciertas configuraciones se recomienda, por seguridad, que el servidor en el que se ejecuta ISA Server no pertenezca a un dominio. Un ejemplo de esto podría ser la implementación del ISA Server como front-end en una configuración back-to-back de Firewalls. En estos casos no podemos contar con los protocolos de autenticación tradicionales como Kerberos o NTLM pero podemos usar protocolos alternativos como RADIUS, que ya era soportado desde la versión ISA Server 2004. En esta versión 2006 tenemos una alternativa que es la de usar el protocolo LDAP para contactar a un servidor LDAP, como lo es un Domain Controller con Active Directory, y requerir la autenticación necesaria para los usuarios aunque el ISA Server no pertenezca al dominio. También podemos elegir usar el protocolo LDAPS para proteger la comunicación establecida con el servidor LDAP.

5) *VPN Wizard:* muchos de nosotros que hemos utilizado la versión de ISA Server 2000, recordaremos la existencia de un wizard para establecer una conexión VPN Site-to-Site configurando al servidor local. El wizard generaba un archivo incluyendo la configuración realizada para que pudiera ser importada en el servidor remoto y ser muy fácilmente configurado. Esta funcionalidad no estaba disponible en la versión 2004 pero ahora nuevamente la tenemos en la versión 2006.

6) *Exchange 2007 Support:* es posible publicar servidores Exchange especificando su precisa versión, entre las cuales está contemplada la nueva versión Exchange 2007 (figura 3).

7) *Flood Mitigation:* se incorpora una funcionalidad para contrarrestar los ataques de flooding, permitiendo limitar el número de sesiones concurrentes TCP o UDP por dirección IP, el número de requerimientos HTTP por minuto por dirección IP, el número de conexiones TCP por minuto por dirección IP, y algunas restricciones más. Hay que considerar el tráfico normal de nuestras aplicaciones para que las comunicaciones originadas por ellas no sean consideradas flooding, y de esa manera ser bloqueadas. De ser así habrá que configurar estos valores para que nuestras aplicaciones funcionen correctamente.

8) *BITS caching:* los archivos que se bajen desde Internet utilizando BITS ahora pueden ser cacheados utilizando esta funcionalidad. En cualquier regla de caching que creamos podemos habilitar el almacenamiento en cache de archivos bajados por BITS. Un ejemplo de archivos que se bajan utilizando la tecnología de BITS son las actualizaciones del sistema operativo, que podría bajar el cliente de Automatic Updates de cada estación de trabajo. Con esta función estamos mejorando el rendimiento que obtienen los clientes y evitando malgastar el ancho de banda de Internet.

9) *Http Compression:* el wizard para crear Web Listeners permite configurar al ISA Server para comprimir el contenido Web enviado a los clientes, en el caso que éstos lo requieran.

10) *Diffserv:* o también denominado Quality of Service, permite categorizar el trafico enviado por el ISA Server, escaneando las URL o dominios y asignándole a los paquetes bits de Diffserv.

Características mejoradas

1) *Outlook Web Access Publishing Wizard:* este wizard permite hacer la publicación de las tecnologías Web, como OWA, RPC sobre http, OMA y ActiveSync, realizando todos los pasos de publicación sin tener que hacerlos por otros medios, desde elegir el tipo de servidor Exchange, configurar las conexiones de SSL desde el ISA Server al servidor Exchange, elegir o crear el Web Listener adecuado, y configurar la delegación de credenciales.

2) *Easy-to-use wizards:* se agregaron nuevos wizards específicos para la publicación de servidores de Windows Sharepoint Services, Exchange y sitios Web en general (figura 4). De esta manera podemos publicar a un servidor de Windows Sharepoint Services evitando hacerlo manualmente como debía hacerse en versiones anteriores de ISA Server.

3) *Certificate Management:* para la creación de conexiones seguras desde Internet al ISA Server, a través del protocolo SSL, es necesario instalar certificados digitales. Ahora se

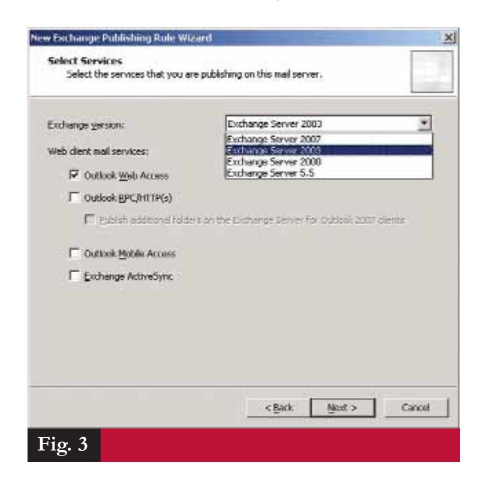


Fig. 3

pueden asignar distintos certificados digitales por cada Web Listener o también por cada dirección IP del ISA Server que utilice el Web Listener. Lo único que hay que tener en cuenta es que no se puede asignar más de un certificado digital a una misma dirección IP. Para la selección del certificado dispondremos de una consola de selección y verificación de certificados, de donde se podrá elegir el certificado, verificar su validez y ver el nombre del servidor CA. Un detalle de esta consola es que aquellos certificados que se encuentren inválidos serán resaltados con una cruz en rojo.

4) *Authentication:* sin lugar a dudas uno de los grandes cambios es el soporte incorporado de distintos esquemas de autenticación. Aquí podemos dividir el mecanismo de autenticación en tres fases. La primera fase es la de solicitar las credenciales al usuario, la segunda fase es la de validar esas credenciales presentadas, y la tercera es la de poder delegar esas mismas credenciales a los servidores publicados. Vamos a ver con qué posibilidades contamos para cada una de estas tres fases.

Para la presentación de credenciales del usuario, dependiendo del tipo de Listener configurado, tenemos las siguientes opciones:

a) HTML Client Certificate Authentication: utilizado para autenticar a través de certificados digitales que el usuario posea;

b) HTTP Authentication: en esta opción están disponibles las tradicionales Basic, Digest e Integrated Authentication;

c) HTML Form Based Authentication: es una nueva forma que posee el usuario para presentar sus credenciales, es decir, a través de un formulario html utilizado para no solamente validarnos al querer acceder a un sitio OWA, como se podía hacer en la versión anterior, sino también a cualquier sitio Web en general; y

d) No Authentication: cuando no requerimos de autenticación por parte del usuario.

Una vez que el usuario presenta sus credenciales, a través de alguno de los mecanismos anteriores, es necesario que el ISA Server pueda validarlas. Para esta función también se cuenta con distintas maneras de validación:

a) Active Directory

b) Active Directory vía LDAP

c) RADIUS (OTP)

d) RADIUS

e) RSA SecurID

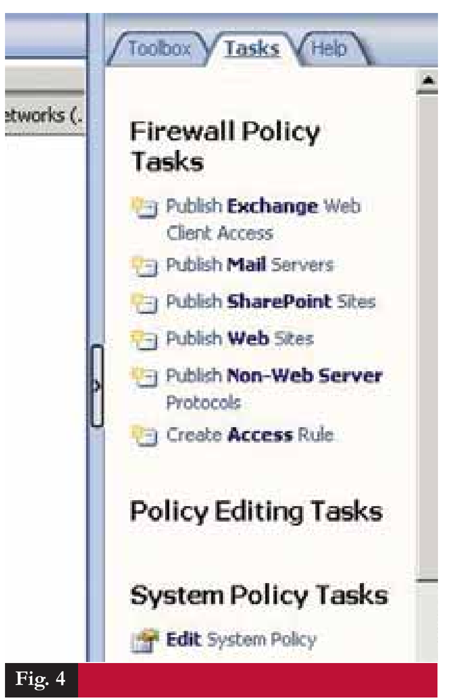


Fig. 4

Por último, las credenciales también pueden ser delegadas al servidor publicado y así evitar al usuario de tener que colocar las credenciales otra vez. En la versión 2004 de ISA Server existía la posibilidad de delegar usando la autenticación básica (Basic Authentication), pero esta manera tiene ciertas desventajas desde el punto de vista de la seguridad, ya que las credenciales son transmitidas sin encriptación alguna. En esta nueva versión disponemos de los siguientes mecanismos de delegación:

a) Basic Authentication

b) NTLM Authentication

c) Negotiate (Kerberos/NTLM)

d) Kerberos constrained delegation

5) *Forms-based authentication:* uno de los mecanismos para que el usuario presente sus credenciales es a través de un formulario html. En la versión 2004 de ISA Server esta opción estaba disponible solo para el sitio Web del OWA, pero en la nueva versión esta disponible para cualquier sitio Web publicado. Además, este formulario html puede ser reemplazado por un formulario personalizado para reflejar la identidad de la organización (figura 5).

6) *Session management:* muchas de las características se basan en la utilización de cookies para establecer las sesiones de los usuarios. Ejemplo de esto es la característica de single sign-on o la publicación de un sitio Web utilizando una granja de servidores.

7) Link translation: esta característica permite reemplazar nombres de sitios internos por nombres que los usuarios de Internet puedan resolver. De lo contrario un usuario de Internet recibiría un error al querer acceder a un sitio utilizando un nombre interno. En



Fig. 5

esta versión esta característica se encuentra activada automáticamente para toda regla de publicación Web.

Conclusión

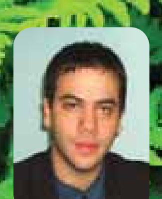
En el caso que queramos probar el producto podemos bajar del sitio Web de Microsoft una versión final de prueba de 180 días de validez, tanto de la versión Standard Edition como de Enterprise Edition.

Para concluir podríamos decir, según el aspecto visual de la interfase gráfica, que muchos se podrían confundir pensando que se trata de la versión ISA Server 2004, y debido a esto concluirían que en vez de llamarse ISA Server 2006 debería llamarse ISA Server 2004 R2. Pero más allá de toda discusión sobre el nombre que debería llevar, en lo que podemos coincidir es en que las funcionalidades agregadas y mejoradas son más que interesantes, aportando una mayor cantidad de posibilidades de configuración haciendo más potente al Firewall de Microsoft. ●

Mejoras

Con respecto a la versión anterior, el ISA Server 2007 trae características mejoradas en cuanto a Certificate Management, necesaria para la creación de conexiones seguras desde Internet al ISA Server; Autenticación, en donde se solicitan las credenciales al usuario, se validan esas credenciales y se delegan a los servidores publicados; Session management; Link translation, que permite reemplazar nombres de sitios internos por nombres que los usuarios de Internet puedan resolver; Forms-based authentication; Easy-to-used wizards y Outlook Web Access Publishing Wizard que permite la publicación de las tecnologías Web.

Windows Vista Group Policies



Por: **Ariel Giarratana**
Senior Trainer
MCSE + Security

Continuando con la nota número III de Windows Vista no podíamos dejar de lado un tema que sin duda merece una revista aparte: Las Group Policies. En este artículo analizaremos qué son las group policies, cómo se administran, y cuáles son las novedades tanto para Windows Vista como para Longhorn Server.

¿Qué son las Políticas de Grupo?

Las políticas de grupo son archivos que contienen seteos que un administrador puede aplicar a máquinas y usuarios locales o de un dominio. Podríamos dividirlas en Políticas locales (Local Group Policies) y Políticas de dominio (GPO´s para los amigos). Las local group policies se guardan localmente en cada máquina (%systemroot%\system32\group policies) y hasta Windows XP y 2003 aplican a todos los usuarios de esa máquina. Es decir, que si abro la consola gpedit.msc (editor de las políticas locales) y configuro que se oculten los íconos del desktop y que no se pueda acceder al panel de control, esto se aplicará a cualquier usuario que se loguee en esa computadora (incluso al administrador). A partir de Windows Vista, ya podemos asignar políticas locales diferentes para los distintos usuarios que se autentiquen en la PC.

Las GPO´s en un entorno de dominio (que se guardan en la carpeta Sysvol en los controladores de dominio), pueden aplicar a nivel Site, Domain y Organizational Unit ("SDOU" machete para el examen) en donde los settings configurados a diferentes niveles que se "opongan", siguen la siguiente regla:

Las de site sobrescriben a las local; las de domain a las de site, y las de OU a las de domain.

Las computadoras y usuarios a la hora de validarse, aplicaban los seteos efectivos de las GPO´s asignadas.

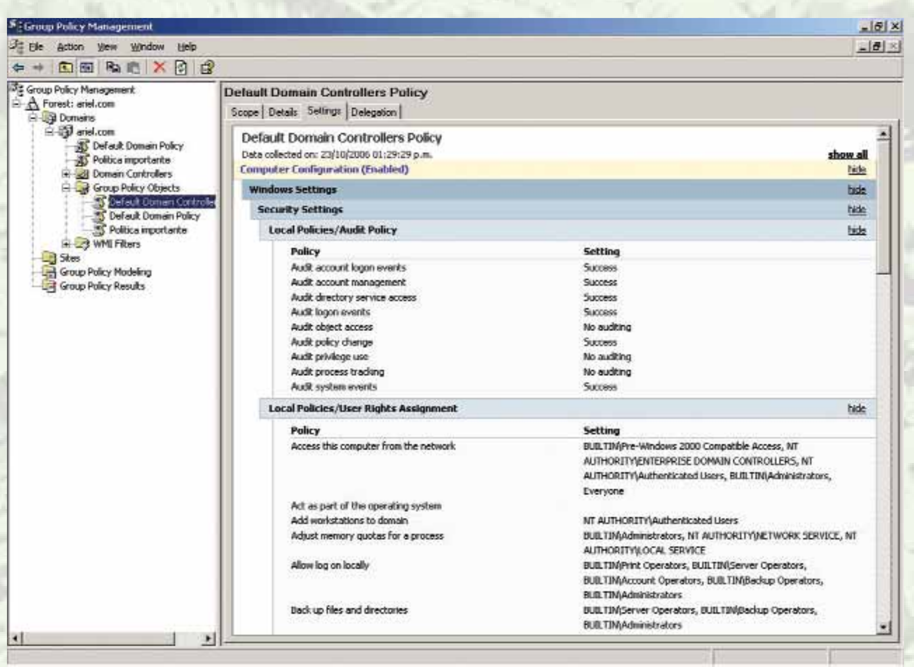
Haciendo un poco de historia, ya desde Active directory 2000, podíamos hacer cosas fantásticas con las GPO´s. Desde configurar casi por completo el desktop de los usuarios, hasta instalar software remotamente, pasando por seteos como configuraciones de seguridad, políticas de IPsec, Auditoría, redirección de carpetas, etc, etc, etc.

Más tarde, y no conformes con eso, con Active directory 2003 se agregaron nuevas políticas (cuenta con unas 1800 en total por default) y además nuevas funcionalidades con respecto a la aplicación de las mismas de la mano de los filtros WMI (en donde yo podría tranquilamente asignar office 2003 a todas las computadoras de mi dominio pero con la condición de que tengan más de un giga de espacio libre en disco, o más de 128 megas de ram, o instalar un parche sólo si está corriendo determinado servicio).

Si bien funcionan excelentemente, y casi nadie se anima a arrojar quejas a esta tecnología que le está ahorrando horas y horas de trabajo al hacer configuraciones a gran cantidad de usuarios y máquinas, se le pueden encontrar algunos "problemas".

Analicemos: Cada objeto de política de grupo que creamos tiene asociado una serie de archivos con extensión .adm conocidos como templates administrativos. Estos templates tienen la funcionalidad de extender los seteos de la política. Cada archivo .adm nos ofrece una serie de seteos (que modifican la registry) y ocupan cerca de 4 mb. Con lo cual, el hecho de crear por ejemplo, 20 nuevas gpos, origina 80 mb de replicación entre los controladores de Dominio.

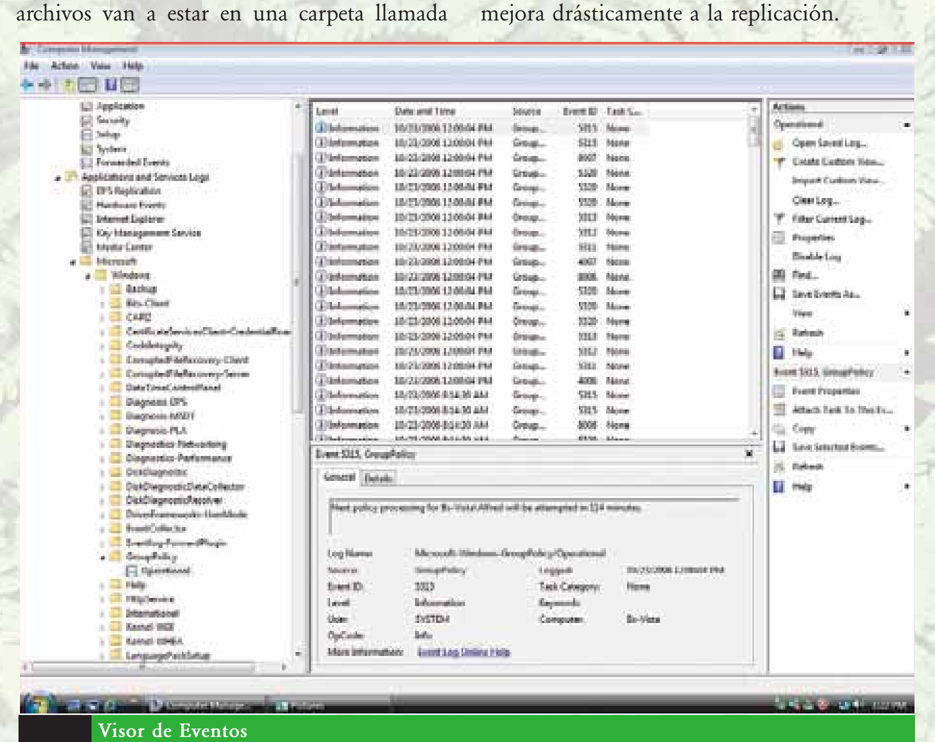
Y si tenemos en cuenta que hay un set de archivos adms para cada idioma, el hecho de tener un dominio con controladores de Dominio en 4 países con diferentes idiomas, multiplicaría por 4 el tráfico de replicación.
El servicio encargado de la replicación de la carpeta Sysvol (que contiene las políticas, adms y scripts) es FRS (File Replication Service).
FRS trabaja replicando todo archivo creado dentro de la carpeta sysvol de cualquier controlador de dominio, al resto de los controladores de dominio, y si alguno sufre una modificación también es replicado en forma completa. Este es un gran problema ya que este servicio no es demasiado parametrizable. Uno no puede definir un schedule de replicación independiente ni definir el ancho de banda para el mismo. Otro problema que agobiaba a los administradores era la dificultad que había para administrar las políticas. Y es por eso que apareció la GPMC (group policy management console). Una consola que se instala aparte (descargándola gratuitamente del sitio web de Microsoft) que nos facilita enormemente la administración de políticas. La cual nos permite hacer cosas como:
- Group Policy Modeling (para analizar qué políticas y seteos efectivos aplican a computadoras y usuarios de una OU, o a determinados usuario y máquina del Active directory).
- Ver en forma más sencilla las políticas (todas desde un contenedor), y poder ver sólo los settings configurados (algo muy práctico ya que normalmente no configuramos ni la décima parte de los settings que hay); también ver a qué contenedores aplican para saber a quienes va a afectar cuando modifiquemos un seteo de esa GPO.
- Manejar los filtros WMI
- Aplicar las políticas a los Sites, Domains, y OU´s en forma sencilla con un simple drag & drop.
- Hacer Backups y Restores de las políticas de una forma increíblemente sencilla.
Si bien la GPMC soluciona este problema, tenemos que estar pendientes de instalarla en toda máquina en la cual administremos las GPO´s y además descargarnos los parches y/o services packs.
Otro punto a tener en cuenta es que uno de los métodos para verificar conectividad entre el cliente y el domain controller para aplicar las políticas es a través del comando Ping. Y muchas veces el tráfico ICMP está filtrado por firewalls. Lo cual también representa un problema.
Y un punto más que los administradores consideran en contra, es la dificultad que hay para encontrar y entender los logs de las políticas. Estos se guardan en userenv.log y realmente a veces se pone difícil entender qué significan. Y en el Event Viewer en el origen de los registros se ve userenv, y no group policy con una buena y clara descripción.
Afortunadamente, Windows Vista y Longhorn Server están cada vez más cerca de salir al mercado, y con todo esto resuelto.

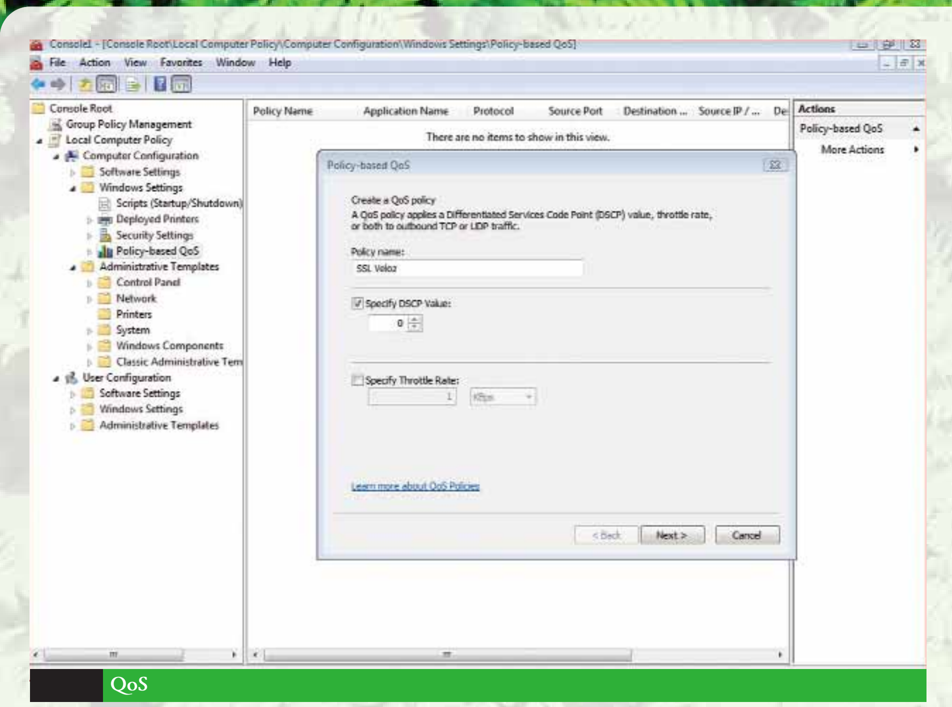


Group Policy Management

Lo Nuevo en Longhorn y Vista

El formato de archivo .adm ahora es reemplazado por .admx. Este es un archivo basado en xml con un lenguaje neutral (contiene seteos iguales para todos los idiomas). Estos archivos van a estar en una carpeta llamada Policy Definitions en todos los controladores de dominio. Y para cada GPO que utilice seteos en diferentes idiomas va a haber archivos .adml (que serán los propios del lenguaje).
Además la replicación ya no se hará más por FRS, sino que pasará a manos del evolucionado DFS (Distributed File System), en donde podremos establecer un schedule de replicación y utilización de ancho de banda. Además, la replicación será sólo de cada seteo modificado de la política. Sin duda todo esto mejora drásticamente a la replicación.


Visor de Eventos



QoS

Para la detección del vínculo para la aplicación de políticas se utilizará un nuevo servicio llamado Network Location Awareness (NLA), con lo que se consigue independizarse del comando ping para la correcta aplicación de las políticas.

Este servicio podrá detectar el enlace caído, o una baja en el ancho de banda para saber si debe aplicar o refrezcar ninguno, algunos o todos los seteos de las políticas. Ahora la GPMC viene instalada por default y se le podrán aplicar los parches y services packs desde windows update. A partir de Windows Vista los logs de group Policies aparecerán en el event viewer con el source Group Policy y una mejor descripción del evento.

Hasta Windows XP el servicio Winlogon era el encargado de aplicar las políticas, pero también de la validación del usuario, máquina e inicio de la interfaz entre otras cosas.

A partir de Windows Vista existe un nuevo servicio llamado “Group Policy Service” que está encargado exclusivamente de la aplicación de políticas.

Y todo esto se traduce en:

- Un servicio más eficiente
- Menos reinicios
- Menor uso de memoria
- Mejora de la performance

Y ahora con Windows Vista y Longhorn Server el número de settings configurables por GPO asciende a -3000!

Por ejemplo, aparecieron políticas como:

Restricciones para la instalación de dispositivos USB: podremos restringir la instalación de cualquier dispositivo y opcionalmente exceptuar alguno/s, o instalar cualquiera excepto el que definamos. Y también se puede configurar que un administrador tenga la posibilidad de sobrescribir localmente estos seteos.

QoS: se podran definir políticas de calidad de servicio en donde le podremos dar prioridad o asignar ancho de banda al tráfico de red que querramos. En donde podremos definir, IP o red de origen y destino, Puertos de origen y destino, Protocolos y Servicios.

UAP: User Account Protection se configurará a través de las políticas de grupo

IE7: todos los settings del Internet Explorer 7 son configurables desde la registry, con lo cual también pueden ser configurados por políticas. Ya vienen los ADMX por default para poder configurar cualquier seteo, sin necesidad de agregar nada extra.

Impresoras: se podrán definir impresoras por política basándose en la ubicación del usuario.

BITS: los settings del servicio de ancho de banda inteligente podrán ser configurados por políticas.

Client Help: podremos configurar si la ayuda estará disponibles para los clientes online u offline.

Disk Failure Diagnostics: podría configurar una GPO con seteos de diagnóstico de Falla de disco y linkearla a una OU en donde tengo file servers para anticiparme a cualquier fallo de disco que pueda haber.

Networking Quarantine: gracias a la nueva tecnología de NAP (Network Access Protection) podremos configurar por políticas si la máquina cliente puede ingresar a la red o quedará en una red en cuarentena, evaluando el estado de la misma (ejemplo: si tiene parches de seguridad instalados, antivirus actualizado, etc).

DVD Video Burning: podremos definir si se puede o no grabar DVD´s.

Qwave: por políticas podremos configurar este servicio que mejora la experiencia de los usuarios que utilizan aplicaciones multimedia en tiempo real, adaptando los seteos al ancho de banda disponible.

Y además políticas de Antivirus, MMTP, Security Protection, Shell Application Management y más...

Conclusión

Se le ha logrado sacar más brillo a las Políticas de grupo agregando cientos de seteos adaptados a las nuevas tecnologías y necesidades, y puliendo aspectos funcionales como la creación de nuevos servicios para la aplicación más efectiva de las mismas, mejorando la replicación, auditoría y detalles como una GPMC integrada. Creo que en este caso, no se les ha escapado nada y realmente tienta a más de uno a implementar esta plataforma. ●

Antivirus
BITS
Client Help
Disk Failure Diagnostics
DVD Video Burning
MMTP
Networking Quarantine
Security Protection
Shell Application Management
UAP

Fundamentos de Networking

La Capa de Enlace

La Capa de Enlace de Datos (capa dos del modelo de referencia OSI) trabaja a nivel de tramas. Entre otras funciones, se encarga de la detección y corrección de errores, y de proveer los mecanismos necesarios para el direccionamiento físico.

Miguel F. Lattanzi
Ingeniero en Telecomunicaciones (IUPFA)

Juan M. Urti
Ingeniero en Telecomunicaciones (IUPFA)

Nota #2 de 5 Serie

1- La Capa Física.

2- La Capa de Enlace: VLAN, Spanning Tree, Bridges y Switches.

3- La Capa de Red: Direccionamiento IP, Protocolos de Enrutamiento, Routers.

4- Tecnologías de WAN: Fundamentos de BGP, Concepto de VPN, VPN basadas en MPLS.

5- Management y IP QoS: SNMP, Prioridades y Reserva de Recursos, Manejo de Colas.

Introducción

La capa de enlace de datos es la segunda capa del modelo de referencia OSI (Open System Interconnect). Como todas las demás capas de este modelo básicamente tiene que ser capaz de enviar y recibir datos –a nivel de capa de enlace se habla de tramas– entre la capa 2 del host transmisor y la del host receptor, según el principio de adyacencia lógica. Además es necesario que tenga la capacidad de poder traducir y enviar la información de su capa inmediatamente superior hacia su capa inmediatamente inferior y viceversa. En el origen se ocupa de fragmentar las tramas en ráfagas de bits y de entregárselos a la capa física para que ésta pueda enviarlos a través del medio hacia su destino. Cuando los datos arriban al destino la capa física envía a su capa inmediata superior las ráfagas de bits que le llegan. La capa de enlace comienza a recibir los bits y los barre para poder ir verificando la integridad de los datos y armar las tramas, que luego enviará a su capa superior, la capa 3 –capa de red–.

Al mismo tiempo, la capa de enlace de datos se encarga de realizar operaciones de verificación y corrección de errores de las tramas de datos y provee los mecanismos necesarios para llevar a cabo el direccionamiento físico por medio del uso de direcciones MAC (Media Access Control).

Debido a las funciones que cumple y las facilidades que provee esta capa se puede tener una idea de su gran importancia.

Adyacencia Lógica

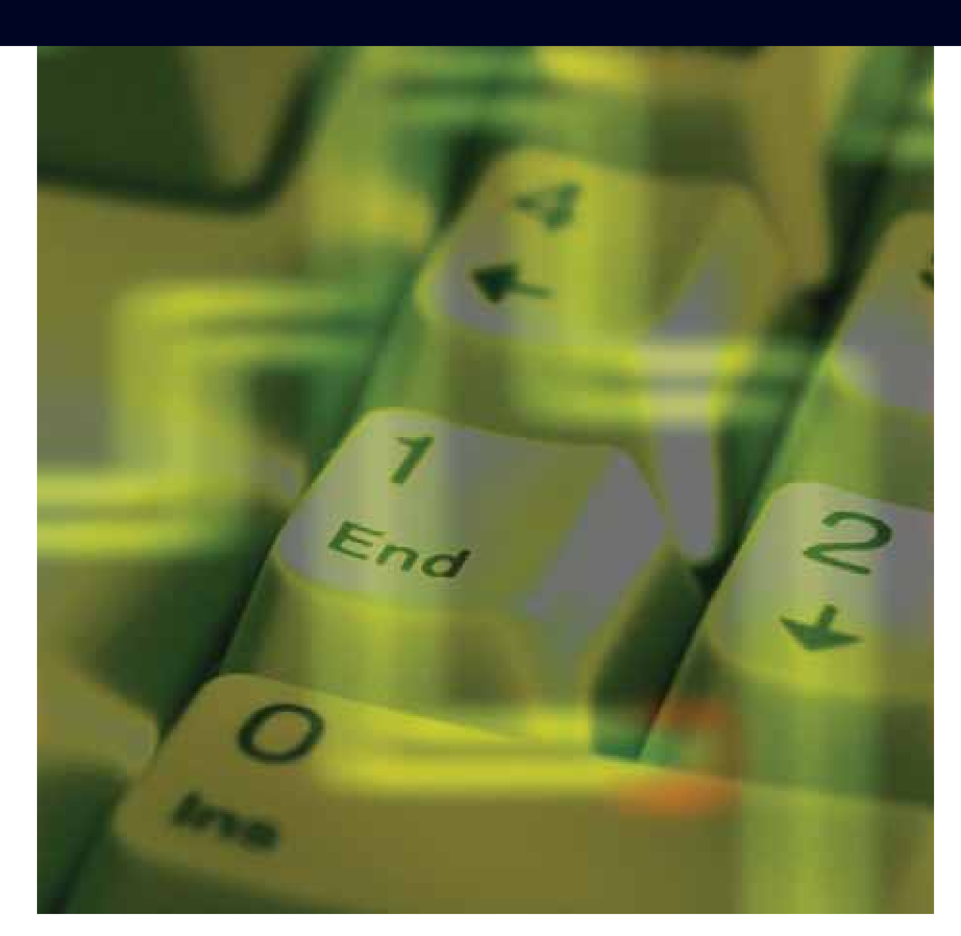
Es la capacidad aparente que poseen las capas del mismo nivel, de un host de origen y un host de destino, de comunicarse entre sí de forma directa cuando en realidad se realiza un procesamiento de los datos en forma descendente (desde las capas superiores hacia las inferiores) en el extremo transmisor y viceversa en el extremo receptor.

Direcciones Físicas

Como se mencionó anteriormente, el direccionamiento físico hace uso de las direcciones MAC para poder enviar tramas entre los distintos hosts. Estas direcciones MAC están compuestas de seis segmentos de 8 bits representados típicamente en formato hexadecimal, de los cuales los primeros tres corresponden a la identificación del fabricante de la NIC (Network Interface Card) –véase referencia [3]– y los últimos tres a la dirección física propiamente dicha. Las direcciones MAC son únicas a nivel mundial y cada fabricante tiene sus propios rangos, para no correr el riesgo de duplicaciones.

Una dirección MAC típica tiene el siguiente aspecto: 00:03:47:17:FF:A5, tal como se mencionó 00:03:47 corresponde al fabricante de la tarjeta de red y 17:FF:A5 a la dirección en sí misma. La trama Ethernet tiene dos campos de 6 Bytes cada uno en donde se colocan las direcciones MAC de origen y destino, éstos son SA (Source Address) y DA (Destination Address), como puede verse en la figura 2. Los dispositivos de capa de enlace utilizan estos campos para confeccionar sus tablas de direccionamiento y conocer así los hosts conectados a cada puerto.

Todos los dispositivos de capa 2 que estén conectados entre sí formaran parte del mismo dominio de difusión de MAC. Se entiende por dominio de difusión de MAC al que esta formado por todos los hosts capaces de recibir tramas de broadcast (difusión) de MAC generadas por otro host de origen.



Tipos de Membresía

La membresía es el criterio por el cual se agrupan los terminales que van a pertenecer a la misma VLAN. Básicamente los modos de pertenencia pueden ser estáticos: cuando el administrador asigna una VLAN a un puerto o dinámicos: cuando se emplea un servidor VMPS (VLAN Membership Policy Server), que se encarga de asociar una VLAN con una MAC Address. Existen otras formas de membresía, como por ejemplo por IP y MAC Address.

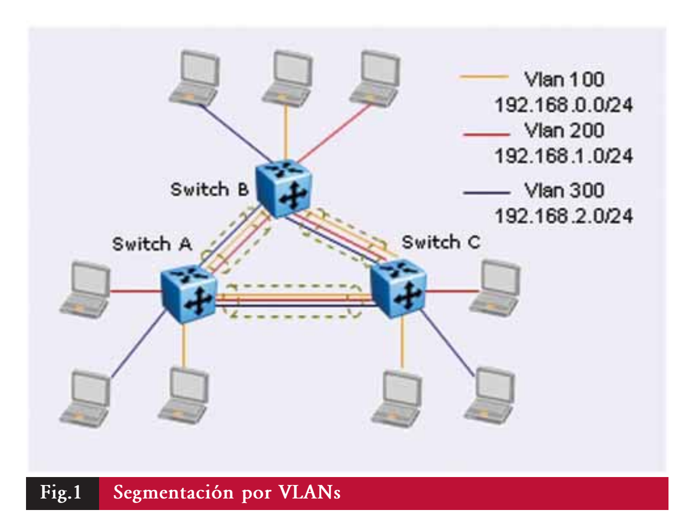


Fig.1 Segmentación por VLANs

VLANs

Los Switches de capa 2 han solucionado el problema de poseer en el mismo dominio de colisión a todos los terminales que se encuentran conectados al mismo medio de acceso (lo cual es un problema inherente a la capa física), ya que ahora cada puerto representa un dominio de colisión distinto. Pero, inicialmente, no podían minimizar los dominios de broadcast, por lo que si un terminal deseaba enviar una trama de difusión, ésta era recibida por la totalidad de los dispositivos de ese dominio. Lo cual generaba tráfico innecesario en ciertas áreas de la red, una solución posible era introducir routers para segmentar estos dominios.

El estándar IEEE 802.1q introduce el concepto de VLAN –Virtual LAN– con el cual a los switches se les incorpora la capacidad de segmentar el tráfico de difusión por grupos de terminales. Cada VLAN funciona como una LAN física distinta, es por ello que el tráfico entre las mismas es aislado. Básicamente una VLAN consiste en agrupar a los dispositivos bajo algún criterio de selección denominado membresía. Una VLAN puede extenderse por varios segmentos LAN y, además, cada una debe estar en una subred IP diferente.

Con esta nueva aplicación una empresa puede segmentar sus redes por sectores, sin importar la ubicación física de los host ni tampoco a qué Switch se conectan. Esto se debe a que, como dijimos antes, las VLANs pueden ser propagadas a lo largo del Backbone de la red. Esta situación puede observarse en la figura 1.

Por medio de las VLANs ahora podemos controlar el tráfico de difusión evitando la necesidad de instalar routers. Es importante mencionar que para que un terminal que pertenece a una VLAN se comunique con otro que se encuentra en otro segmento virtual debe existir un router o un Switch con funcionalidades capa 3 capaz de enrutar los paquetes IP; recordemos que cada VLAN se encuentra en una subred IP diferente. En redes de tamaño mediano es común que las VLANs se propaguen por varios Switches con el objetivo de extender el segmento a varios lugares físicos y, por tal motivo, nos introduciremos en un concepto muy importante: trunking.

Las interfaces de los dispositivos LAN de capa 2 pueden estar configuradas como Access cuando el puerto pertenece a una sola VLAN, o bien como trunk, cuando en el puerto son permitidas un conjunto de VLANs. Los puertos trunk tienen como objetivo transportar el tráfico entre diversos switches, marcando las tramas con una etiqueta, en la cual se encuentra el valor de la VLAN a la que pertenece el puerto.

El método que emplea el Switch para realizar esta tarea se denomina encapsulación, y por excelencia el más utilizado es el IEEE 802.1q.

El estándar IEEE 802.1q le agrega a las tramas Ethernet una etiqueta de 4 Bytes, como se puede apreciar en la figura 2.

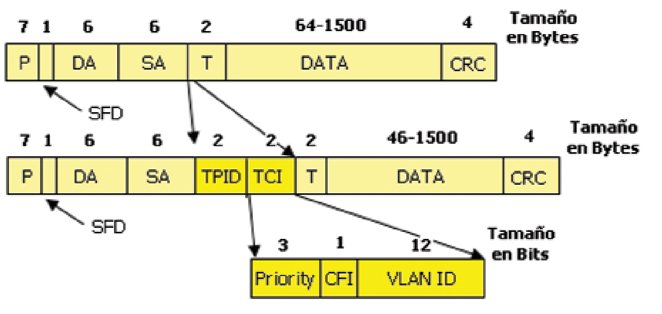


Fig.2 Trama IEEE 802.1q


like.no.other™
SONY
TAZA TERMÓMETRO
DE LOS TANTOS INVENTOS
QUE NO PUDO SER POSIBLE
POR LA PÉRDIDA DE INFORMACIÓN.
520 GB*
Advanced
Intelligent
Tape
SU INFORMACIÓN MUCHO MÁS SEGURA.
Sony AIT (Advanced Intelligent Tape) es la mejor tecnología
para el Back Up de su empresa.
La capacidad va desde 20 GB a 520 GB*, brindándole así
toda la seguridad y confianza que usted necesita. Desde
Pymes a grandes empresas, AIT es escalable de acuerdo
a la necesidad del usuario.
*Compresión 2.6:1.

Esta etiqueta de 4 Bytes se inserta luego de la dirección de origen y como muestra la figura 2 se divide básicamente en dos partes: TPID –Tag Protocol Identifier– el cual indica qué protocolo de encapsulación se está empleando (0x8100 para IEEE 802.1q), y TCI –Tag Control Identifier–. El campo TCI consta de 16 bits, los primeros 3 bits se denominan Priority, empleándose para priorizar tramas (este campo se marca para QoS); el bit siguiente se llama CFI –Canonical Format Identifier– y es puesto en cero cuando trabajamos en entornos Ethernet (indica cómo se debe leer la trama); y los restantes 12 bits indican el VLAN ID, o sea, básicamente el número de VLAN. De este número observamos que podemos obtener 4096 VLANs, aunque se encuentra en proceso de estandarización por la IEEE, aumentar el número total por medio de Q-in-Q (véase NEX IT #27, "Redes Metro Ethernet").

Debemos aclarar que para IEEE 802.1q la VLAN nativa (por lo general la número 1) no se etiqueta en ningún Switch, por lo que los terminales que no estén en ninguna VLAN estarán por defecto al menos en la VLAN 1 internamente y serán capaces de leer las tramas que no arriben etiquetadas.

Spanning Tree Protocol

Uno de los objetivos principales a la hora de diseñar una red es proveer a esta de la mayor disponibilidad y redundancia posible, disminuyendo los puntos críticos de falla y llevando la confiabilidad al máximo.

A pesar de ello, las topologías redundantes traen consigo algunas consideraciones a tener en cuenta. Supongamos que tenemos una serie de Switches conectados por medio de vínculos redundantes como muestra la figura 3.

Consideremos que la PC1 y la PC2 recién se conectan a la red. Si el primer terminal desea comunicarse con la otra PC, este colocará la IP destino en el campo correspondiente del paquete IP, y encapsulará esto en el campo de datos de la trama Ethernet. Como la PC2 recién se conectó a la red, es probable que la PC origen no conozca la MAC Address destino, y por lo tanto, a la PC1 no le quedará otra opción que realizar una broadcast de capa 2, colocando como dirección destino FF:FF:FF:FF:FF:FF en la trama antes de ser enviada.

Cuando la trama llega a los Switches A y C, estos la retransmiten a todos los puertos –menos el origen–. El Switch B recibirá la trama desde la conexión A y la reenviará a la conexión B, pero luego recibirá desde la conexión B otro broadcast –en realidad el mismo– proveniente del Switch C y lo enviará a la conexión A, produciéndose así un loop de nivel de enlace –a este fenómeno se lo conoce como tormenta de broadcast– que además de volver inestables a las tablas de MAC, inunda la red de tráfico, proceso que se conoce como flooding.

Fig.3 Loop lógico entre Switches

RSTP y MST

Rapid STP es el estándar IEEE 802.1w introducido para reducir los tiempos de convergencia. Posee muy pocas diferencias con el 802.1D y la filosofía de trabajo es la misma. MST permite agrupar un número de VLANs bajo la misma instancia de STP, permitiendo por ejemplo que un puerto esté bloqueado para una VLAN, y como forwarding para otra.

Para resolver este inconveniente la IEEE desarrolló un protocolo denominado Spanning Tree Protocol (STP).

STP es el estándar IEEE 802.1D y tiene por objetivo hallar por medio de un algoritmo un único camino entre dos estaciones de una red, evitando de esta manera los loops.

Dentro de la topología de la red todos los puertos de los Switches adquieren roles y estados. Para poder mantener la topología actualizada cada Switch que utiliza STP envía cada 2 segundos una trama denominada BPDU –Bridge Protocol Data Unit–, que transporta la información del Switch, sus puertos, el número de secuencia de la trama y los dos parámetros relevantes a la hora de elegir los roles de las interfaces: el Bridge ID y el Path Cost.

El Bridge ID –BID– es un campo del BPDU con una extensión de 64 bits que se compone de dos o tres partes, según el modo de STP que se este empleando. La primera parte consta de 16 bits, denominada Bridge Priority, y se emplea para determinar la prioridad del Switch dentro de la topología (los valores van desde 1 a 32768). Debemos aclarar que para las versiones más modernas de STP, como los son Rapid STP o MST (Multi-Instance Spanning Tree), a este valor de prioridad se lo ha disminuido a 4 bits, dejando los restantes para la identificación de la VLAN. La segunda sección del BID es la MAC Address, compuesta como dijimos por los restantes 48 bits.

El Path Cost representa la suma de todos los anchos de banda de los enlaces hasta el Root Bridge. Los costos, luego de la revisión de la norma en el 2003, son: 2 para 10 Gbps, 4 para 1 Gbps, 19 para 100 Mbps y 100 para 10 Mbps.

Al iniciar STP en la red, por la misma comenzarán a circular los BPDUs y, en base al BID y al Path Cost, los Switches y sus puertos adquirirán roles.

El primer rol a elegir es el Root Bridge (RB), el cual poseerá todos sus puertos en estado Forwarding o envío –osea enviará tramas por todos sus puertos–. Este RB es único en el dominio de difusión y posee el BID más bajo o la menor dirección MAC.

El segundo rol es el Root Port (RP), habiendo un RP por cada No RB. Para que un puerto de un Switch se encuentre en este estado debe tener el Path Cost más bajo hacia el RB y su característica principal es que se encontrará en forwarding.

Luego se define el rol de Puerto Designado (DP), que son puertos que tienen el costo más bajo hacia el RB pero no están directamente conectados a su segmento. Estos puertos a diferencia de los no designados –NP, el cuarto rol–, están en estado de forwarding. Los puertos NP se encuentran bloqueados y por ende son los que cortan el loop de manera lógica.

Luego de que el algoritmo actúe solo habrá entre dos estaciones un único camino, por lo que la red estará libre de loops de capa 2. Además, debemos mencionar que si STP funciona correctamente los puertos se deberán encontrar en blocking o forwarding.

Una vez que la topología se altera, y hasta que la topología se vuelve a estabilizar, los puertos atraviesan los estados de blocking, listening, learning y forwarding. El tiempo que le demora a STP en recalcular la topología de la red es de 30 a 50 segundos y se denomina tiempo de convergencia.

Bridges y Switches

Los Bridges y los Switches son los dispositivos que proveen conectividad a nivel de capa de enlace, dado que trabajan con tramas de datos y por ende con direcciones MAC. Básicamente se utilizan para separar un dominio de colisión en dos o más dominios, con lo cual se logra tener segmentos de red aislados, que permiten separar el tráfico para que este no se propague a los segmentos que no sean necesarios. Con esto se logra reducir la probabilidad de ocurrencia de colisiones. También es importante mencionar que en el caso de producirse colisiones en un dominio estas solo afectaran a dicho dominio y no se propagarán a otros segmentos de la red.

La filosofía de ambos equipos y el modo de fun-

cionamiento es muy similar, la principal diferencia radica en que los Bridges tienen solamente dos puertos para interconectar dos segmentos de red, mientras que los Switches suelen tener al menos doce o dieciseis puertos. Además, estos últimos tienen más funcionalidades y han evolucionado hasta adquirir capacidades de capa 3, como se mencionó con anterioridad.

Dominios de Colisión

Recordemos que un dominio de colisión está compuesto por todos los hosts que deban competir por los recursos necesarios para enviar la información a través del medio de transmisión.

Manteniendo la línea de tiempo, respecto de la evolución histórica, primero realizaremos el análisis de funcionamiento de los Bridges. Estos son dispositivos de capa 2 que sirven para interconectar dos segmentos de red aislados que pueden o no tener arquitecturas similares. En estos equipos las tablas de direccionamiento son confeccionadas en base a las direcciones físicas MAC de los terminales que se encuentran conectados a cada uno de los segmentos de red.

Los Bridges realizan tres funciones básicas para poder hacer entrega de la información, evitar las colisiones y el tráfico innecesario y aprender las nuevas direcciones MAC para mantener su tabla de direccionamiento actualizada. Para entender mejor estos procedimientos utilizaremos como ejemplo práctico la figura 4.

La funcionalidad de **Forwarding** permite que las tramas de datos sean retransmitidas desde un segmento de red hacia el otro a través del Bridge. Dada la naturaleza de Ethernet cuando el host A se quiera comunicar con el host C enviará una trama de datos que llegará tanto al host B como al puerto P0 del Bridge. El host B al verificar que la dirección MAC de destino (DA) no corresponde con la suya, procederá a descartar la trama. En tanto, P0 aceptará la trama para que el Bridge pueda comparar la dirección MAC de destino con su tabla de direccionamiento. En ésta podrá observar que la dirección MAC de destino del host C (CC:CC:CC:CC:CC:CC) se encuentra relacionada con el puerto P1, por lo tanto la reenviará a través del mismo. De esta manera, la trama de datos alcanzará de forma correcta su destino.

Dirección MAC	Puerto
AA:AA:AA:AA:AA:AA	P0
BB:BB:BB:BB:BB:BB	P0
CC:CC:CC:CC:CC:CC	P1
DD:DD:DD:DD:DD:DD	P1

Fig.4 Funcionamiento de un Bridge

Otra funcionalidad que poseen los Bridges es la de **Filtering**, por medio de la cual se bloquea el tráfico de un mismo segmento de red para que no llegue al otro. Si el host A desea comunicarse con el host B enviará una trama de datos como en el caso anterior, pero esta vez cuando el host B verifique la dirección MAC de destino comprobará que es la suya y aceptará la trama para realizar el posterior procesamiento de la información. En cambio, cuando la trama de datos ingrese por el puerto P0, el Bridge verificará la dirección MAC de destino y encontrará que la misma está asociada al puerto P0, que es el mismo puerto por donde ingresó. Como carece de sentido reenviar la trama al otro segmento de red, la descartará evitando así generar tráfico innecesario, además de disminuir las probabilidades de que se produzcan colisiones.

Por último, y no menos importante, está la funcionalidad de **Learning**. Esta permite que el Bridge pueda aprender las direcciones MAC de los hosts nuevos, que se vayan incorporando a cada segmento de red. El funcionamiento es el siguiente, supongamos que el host A se quiera comunicar con el host D y este último sea nuevo en su segmento. Cuando el Bridge reciba la trama con la dirección MAC de destino de D, no la conocerá porque no está en su tabla de direccionamiento, por lo cual enviará la trama por el puerto P1, esperando que alguien la reciba. Esta etapa es similar al comportamiento de Forwarding, solo que en lugar de enviar la trama por P1 porque conoce la dirección la envía por allí, porque al no conocerla debe asegurarse de que las tramas lleguen a todos los segmentos dado que el host D podría estar conectado en cualquiera de ellos. El host D recibe la trama y contesta, el Bridge revisa las direcciones MAC y se da cuenta de que la dirección de origen no esta en su tabla (la correspondiente al host D), por ende la agrega y la asocia al puerto P1, luego revisa la MAC de destino y como la conoce reenviará la trama por el puerto correspondiente.

Para finalizar la descripción de los Bridges podemos mencionar que existen tres tipos principales: **Transparent**, los cuales permiten interconectar dos segmentos de red de similar arquitectura –dos segmentos Ethernet por ejemplo–, **Translational** que pueden interconectar segmentos de red de distinta arquitectura –un segmento Ethernet con un segmento Token Ring por ejemplo–, dado que tienen la capacidad de realizar la traducción de protocolos necesaria. Estos se suelen utilizar para interconectar segmentos Ethernet a través de un Backbone de alta velocidad, como ser FDDI (Fiber Distributed Data Interface); y **Speed-Buffering** que permiten interconectar segmentos de red de similar arquitectura que trabajen a distinta velocidad de transmisión de datos –un segmento Token Ring que opere a 4 Mbps con otro segmento que lo haga a 16 Mbps–, realizando la adaptación de velocidades adecuada.

Los Switches funcionan de forma muy similar a los Bridges en cuanto al armado de tablas. La diferencia radica en que los Switches generaran una tabla de direccionamiento por VLAN, en la cual colocaran todos los puertos de una misma VLAN. Otra diferencia que éstos poseen con los Bridges son los modos de operación. Los Switches, según los roles que tengan, pueden operar básicamente de dos maneras: **Store and Forward** en donde el Switch recibe la trama de datos, realiza un control de errores y coteja las direcciones MAC para generar las tablas de direccionamiento físico, luego de lo cual reenvía la trama; y **Cut Through** en donde el Switch realiza un barrido de los bits a medida que los recibe y cuando encuentra la dirección MAC de destino reenvía la trama por el puerto que corresponda sin realizar un control de errores. Los Switches de backbone trabajan con Store and Forward para no difundir errores en la red, mientras que los Switches conectados en cascada suelen utilizar Cut Through debido a la baja latencia que introducen. ●

Funcionalidades de los Bridge

El Forwarding permite que las tramas de datos sean retransmitidas desde un segmento de red hacia el otro a través del Bridge. Otra funcionalidad es la de Filtering, por medio de la cual se bloquea el tráfico de un mismo segmento de red para que no llegue al otro. La última, es la funcionalidad de Learning, la cual permite que el Bridge pueda aprender las direcciones MAC de los hosts nuevos, que se vayan incorporando a cada segmento de red. Estas funcionalidades están presentes en los tres tipos de Bridge: Transparent, Translational y Speed-Buffering.

Lectura Adicional

[1] Sportrack M. IP Routing Fundamentals. Cisco Press, 1999.
[2] McQuerry S. Libro de Autoestudio CCNA. Cisco Press, 2da. Edición, 2004.
[3] http://www.standards.ieee.org/regauth/oui/oui.txt
[4] http://www.cisco.com
[5] http://www.ieee.org

LO QUE SE VIENE: WEB 2.0



Ricardo D. Goldberger

Periodista Científico especializado en Informática y Nuevas Tecnologías.

Hace un tiempo que hemos estado oyendo hablar de Web 2.0, Web Semántica y otras nuevas y distintas variantes de la Web, que se caracterizan como "nuevas". Lo cierto es que, al margen de las tendencias que se vislumbran desde el punto de vista del negocio, hay fuertes indicios de que la Web 2.0 no sólo es una realidad, sino que está marcando el camino para el futuro de Internet. Y los tecnólogos, programadores, diseñadores y afines no pueden quedarse afuera.

Según la Wikipedia, "el término fue acuñado por Dale Dougherty de O'Reilly Media en una lluvia de ideas con Craig Cline de MediaLive para desarrollar ideas para una conferencia. Dougherty sugirió que la web estaba en un renacimiento, con reglas que cambiaban y modelos de negocio que evolucionaban. Dougherty puso ejemplos – 'DoubleClick era la Web 1.0; Google AdSense es la Web 2.0. Ofoto es Web 1.0; Flickr es Web 2.0.' – en vez de definiciones, y reclutó a John Battelle para dar una perspectiva empresarial, y O'Reilly Media, Battelle, y MediaLive lanzó su primera conferencia sobre la Web 2.0 en Octubre del 2004".

Y agrega: "En general, cuando nos referimos al término Web 2.0 nos referimos a una serie de aplicaciones y páginas de Internet que utilizan la inteligencia colectiva para proporcionar servicios interactivos en red dando al usuario el control de sus datos".

Si bien algunos identifican a la Web 2.0 con la Web Semántica, para otros, esta última sería la Web 3.0, ya que posee características "inteligentes", o por lo menos de lenguaje natural que la distinguen de la Web actual.

Según Christian Van Der Henst (http://www.maestrosdelweb.com/editorial/web2/), "la Web 2.0 es la representación de la evolución de las aplicaciones tradicionales hacia aplicaciones web enfocadas al usuario final. El Web 2.0 es una actitud y no precisamente una tecnología".

Y de acuerdo a Rodrigo Galíndez (http://www.16bits.net/archivos/que-es-la-web-20/):

- Es un conjunto de servicios, no un software empaquetado.
- Su arquitectura es la participación.
- Es escalable de forma efectiva en costos.
- Sus fuentes de datos y las transformaciones entre ellas son de varios tipos (tecnologías como AJAX, XML, Flash).
- El software o la aplicación puede ser ejecutado en más de un dispositivo (accesibilidad).
- Aprovecha la inteligencia colectiva (tags).

Si bien es casi una perogrullada decir que la Web 2.0 no es una tecnología, lo cierto es que sin una plataforma tecnológica ésta no será posible.

En la página de Van der Henst se lee:

"Algunas tecnologías que dan vida a un proyecto Web 2.0:

- Transformar software de escritorio hacia la plataforma del web.
- Respeto a los estándares del XHTML.
- Separación de contenido del diseño con uso de hojas de estilo.
- Sindicación de contenidos.
- Ajax (Asincronical javascript and xml).
- Uso de Flash, Flex o Lazlo.
- Uso de Ruby on Rails para programar páginas dinámicas.
- Utilización de redes sociales al manejar usuarios y comunidades.
- Dar control total a los usuarios en el manejo de su información.
- Proveer APIs o XML para que las aplicaciones puedan ser manipuladas por otros.

más la recomendación de URL sencillos.

Es evidente que estamos hablando de mucha tarea por delante.

Barracuda por dentro

Conozca cómo funciona y qué hay dentro de uno de los dispositivos más utilizados para evitar el spam en la bandeja de entrada.



Sin lugar a dudas, hoy en día el spam es uno de los temas más preocupantes. Es por esto que anualmente el Network Computing Lab, uno de los sitios más prestigiosos evaluadores de tecnologías/IT/Networking/Internet, se encarga anualmente de analizar las diferentes opciones existentes a la hora de luchar contra el correo no deseado. Pero, ¿cómo lo hacen? Invitan a participar de la prueba, en el Real-World Lab de la Universidad de Syracuse, a 35 vendors especializados en software, antispam, appliance y proveedores de servicios. Para poder calificar y participar, los productos antispam tienen que operar en la frontera de Internet o en el perímetro como gateway del mail e interoperar con cualquier servidor de mail corporativo.

	Barracuda Spam Firewall 300	Vircom modusGate	BorderWare MXtreme Mail Firewall Appliance MX-400 3.1	Sophos PureMessage 4.5
ANTISPAM ACCURACY (30%)	4.4	4	4.8	4.4
ADDITIONAL FEATURES				
Antivirus (5%)	4	4	5	4.5
Attachment filtering (5%)	4	4.5	5	2
Outlook/Exchange Notes/ Domino integration (5%)	2	3	3	1
Quarantine (5%)	5	4.5	2	4.5
PRICE (PER USER, PER YEAR)				
1,000 users antispam, antivirus (10%)	5	4	2	3.5
10,000 users antispam, antivirus (10%)	5	4.5	3	3
ARCHITECTURE (15%)	3.5	4	4.5	4.5
MANAGEMENT/CONFIGURATION				
Distributed administration (5%)	1	4	4	5
End-user controls (5%)	4.5	4	2	4
Reporting (5%)	3	2	5	3.5
TOTAL SCORE (100%)	4.02	3.95	3.92	3.87
A:-4.3, B:-3.5, C:-2.5, D:-1.5, F:<1.5 A-C grades include + or − in their ranges. Total scores and weighted scores are based on a scale of 0-5.	B+	B	B	B

Tabla 1 Extraída de Network Computing Magazzine

	Inbox	Spam	Total	Inbox common	False negatives	False positives	Nonweighted accuracy	Weighted accuracy
Control	210	1338	1548	210	0	0	100.0%	100.0%
Greenview Data	263	1285	1548	202	61	8	95.5%	93.5%
IronPort	291	1257	1548	204	87	6	94.0%	92.4%
Brightmail	291	1257	1548	204	87	6	94.0%	92.4%
BorderWare	292	1256	1548	204	88	6	93.9%	92.4%
Barracuda	260	1288	1548	193	67	17	94.6%	90.2%
Sophos	298	1250	1548	199	99	11	92.9%	90.1%
Espion	261	1287	1548	192	69	18	94.4%	89.7%
Katharion	207	1341	1548	182	25	28	96.6%	89.3%
Vircom	221	1327	1548	184	37	26	95.9%	89.2%
Proofpoint	275	1273	1548	193	82	17	93.6%	89.2%

Tabla 2 Extraída de Network Computing Magazzine

Los parámetros más tenidos en cuenta para la evaluación son los siguientes:

• **Un producto que no necesitara mucho cuidado** ni mantenimiento por parte del staff IT.

• **Implementar un producto de precisión**, que reduzca significativamente el correo no deseado y que nos ahorre tiempo buscando por el correo legítimo que fue catalogado como no deseado por error. Es decir, que evite los falsos positivos.

• **Identificar un producto que se adecue a las necesidades al menor costo posible por usuario.**

A pesar de que los factores descriptos son los principales para calificar a los productos (especialmente precisión), elementos como el precio, la arquitectura, la configuración, el management, control por parte del usuario final, la seguridad y la capacidad como antivirus también son tenidos en cuenta. Con respecto a la precisión el Network Computing Lab hace una diferenciación entre los falsos positivos y los falsos negativos. Consideran que un falso positivo (un correo electrónico solicitado catalogado como spam) es mucho más costoso para la organización que un falso negativo y por esto es más importante que no se catalogue a ningún correo solicitado como spam a que catalogue a un spam como correo bueno.

Durante el 2004 y 2005 (en el 2006 se cambiaron las bases) el ganador por precisión, características adicionales como el correcto filtrado del documento adjunto, el precio y la configuración fue el Barracuda Spam Firewall 300 con una puntuación final de B+ (ver tabla 1).

La tabla 2 muestra la precisión de los diferentes dispositivos sin tener en cuenta su precio pero analizando de un total de 1548 mails cuántos detectó como correo solicitado, cuántos catalogó como spam, los falsos negativos y falsos positivos.

Barracuda Networks Spam Firewall 3002.2.3

Con solo 3 años de existencia el Barracuda Networks Spam Firewall fue el ganador del Editor's Choice por dos años consecutivos. Las razones por las cuales logró un puntaje final de 4.02 son que este appliance frena el 100 por ciento de los correos no deseados sin generar ningún falso positivo. Obviamente no es gratis, pero su costo por usuario es extremadamente bajo, otra característica que importa a la hora de la evaluación. La compañía mantiene bajos los costos mediante la utilización de un harware of-the-shelf y aplicaciones open-source, incluyendo SpamAssassin, corriendo sobre un kernel de Linux. La tecnología detrás del Spam Firewall no es nada nuevo pero funciona, es completamente accesible y es uno de los productos más fáciles de utilizar y administrar. Solo hace falta logearse en la consola, hacerlo correr para es-tablecer la información de IP, y luego conectarlo al aparato a través de la interface Web para terminar la instalación para el test. Se establecen las definiciones de spam y virus para ser actualizado automáticamente a cada hora, pero cada configuración puede ser cambiada de acuerdo a las necesidades.

Una vez que el test finalizó, se deshabilita la configuración original, se activa el escaneo del antivirus y se establece la cuarentena para el spam. Además se deben determinar los parámetros para detectar en el umbral de entrada el posible spam, la cuarentena definida de acuerdo al spam y el eliminado. Esto toma solo tres minutos y no hace falta corroborar con el manual ni llamar para soporte técnico.

Otra de las ventajas es que no hace falta un equipo especial de IT para poder manejar el Spam Firewall eficazmente. Es por esto que generalmente es utilizado por pequeñas y medianas empresas por los bajos costos y la facilidad de uso, pero igualmente también los proveedores de Internet lo utilizan por la licencia por caja y no por usuario.

El Barracuda Spam Firewall posee un dispositivo llamado Exchange Accelerator, que es un buscador de LDAP que puede trabajar con cualquier servidor de LDAP. El Accelerator protege a su servidor de email de los ataques de diccionario a través de una pregunta del LDAP para chequear que el destinatario de un nuevo mensaje tiene una casilla de mail en el servidor de correo electrónico. Si la pregunta del LDAP no es respondida, el appliance genera una NDR (nondelivery report) y devuelve el mail a quien lo envió.

Por estas razones es que Barracuda Spam Firewall es una solución integrada de hardware y software que brinda una solución eficaz de tipo empresarial que incluye todas las características necesarias para eliminar el correo no deseado y proteger completamente el servidor de correo electrónico de cualquier tipo de ataque.

Proofpoint Protection Server 1.5	Greenview Data SpamStopsHere	Brightmail Anti-Spam 5.5	Katharion Anti-Spam for Businesses	IronPort C60	Espion Interceptor 1.3125
4	5	4.8	4	4.8	4.2
4	4	4	5	4	1
4	3	1	3	3	4
1	1	5	1	3.5	1
4.5	1	3	2.5	3	5
2.5	4	2.5	3.5	1	4
3	3	2.5	2.5	2.5	4
5	5	4	5	3.5	2
5	3	1	3	3	1
2	1	4	4.5	3	3
5	3	3.5	2	3.5	3
3.78	3.75	3.62	3.60	3.47	3.26
B	B	B-	B-	C+	C+

Para cada necesidad, un experto

Pablo Corvalan
Gerente de Programas
Socios de Negocios | **Microsoft**

Cada vez que una empresa enfrenta el desafío de incorporar o renovar su tecnología necesita contar con el asesoramiento de un especialista que entienda y responda adecuadamente a sus requerimientos. Conozca las ventajas de contar con los Expertos Certificados de Microsoft.

Los mejores empresarios saben que la inversión más valiosa que puede hacer en su empresa es potenciar el talento de sus colaboradores. En cada rol, en cada proceso las personas son las que hacen la diferencia y crean el valor para los clientes. En este desafío, la tecnología juega un papel fundamental como activo estratégico que permite incrementar los niveles de excelencia, productividad y colaboración de sus equipos.
Esto es muy claro en un mercado como el argentino donde se presentan ciclos muy marcados de crecimiento y recesión. En el ciclo de expansión del negocio necesitamos reaccionar rápidamente al cambio para capturar la oportunidad de crecimiento. Al incorporar en la empresa una plataforma ágil e innovadora habilitamos a las personas a mejorar su productividad, movilidad y capacidad de comunicarse con más clientes.
En estos casos es vital contar con un socio tecnológico especializado que comprenda claramente cuáles son nuestros desafíos de crecimiento y los pueda transformar en soluciones de tecnología. Socios con la experiencia necesaria para encontrar la solución específica que cada escenario de negocio plantea.

Compromiso con la especialización y calidad

En Microsoft sabemos lo importante que es para los clientes encontrar a socios comprometidos con la calidad que puedan dar soluciones. Por eso, hemos estructurado el Programa de Socios de Negocios Certificados que apunta a facilitarles la identificación del mejor aliado para su proyecto particular. Verdaderos especialistas en tecnología y servicios, cuyo expertise está avalado por las certificaciones Microsoft.
Cada certificación es muestra del compromiso de nuestros socios por entrenarse y brindar un servicio de calidad adaptado a cada tipo de escenario. Y un reconocimiento de Microsoft a la especialización y experiencia en el diseño de soluciones basadas en nuestra tecnología.
De este modo construimos una comunidad que permite ofrecer soluciones diferenciadas y de alto valor agregado. Cada uno haciendo lo que mejor sabe hacer, para así minimizar los riesgos de implementación y sacar el mayor provecho de la inversión realizada. Y, por supuesto, asegurar el mejor servicio de post-venta. ●

"Sepa porqué empresas como Cisco, Juniper, Intel, Ebay, Mercado Libre, El Nasdaq, Terra Networks, Telefónica, Time Warner, CNN, ocho de los diez topten ISP del mundo y 4 de las 5 fuerzas armadas de los Estados Unidos utilizan la tecnología de Ironport"

Solucionando los problemas de Seguridad de Correo Electrónico



La seguridad de los mensajes de correo electrónico es una cuestión clave para cualquier organización, sin importar su tamaño. Pero asegurar las comunicaciones a través del e-mail no implica sólo detener el spam y los virus: el correo basura y los programas maliciosos son apenas la punta del iceberg de una problemática compleja.

El correo electrónico es una herramienta vital para el funcionamiento interno y externo de una empresa, de un proveedor de servicios y de hasta un usuario domiciliario. Más allá de los tradicionales métodos de contacto como ser dirección postal, teléfonos fijos y móviles, hoy no falta en ninguna página corporativa ni tarjeta empresarial la dirección de correo electrónico. Es más, la dirección de correo electrónico es hoy día el elemento vital de contacto.

Tal es la dependencia de las personas, proveedores y/o empresas del correo electrónico, que hoy día es el medio favorito de ataque para los hackers y spammers. En realidad, hackers y spammers van de la mano en este negocio como lo mostraremos más adelante.

Pero entrando más en detalle, la Seguridad de Correo Electrónico es un tema mucho más complejo que detener spam y virus, es más, me atrevería a decir que comparado con los problemas de denegación de servicio de correo electrónico, el tema del spam es un mal menor. Casi ninguna compañía de seguridad ha entendido claramente la problemática de ori-



gen de la seguridad de correo. Todos se enfocan en proveer soluciones antispam y antivirus, pero adolecen de una solución completa de seguridad de correo que tiene que ser apuntalada por los siguientes ítems:

Una solución de correo electrónico debe contemplar:

• **No correr sobre un sistema operativo tradicional** (Windows, Linux, etc). Siendo una solución de seguridad de perímetro, no debe estar expuesta a los problemas de seguridad del OS. El Ironport corre sobre un sistema operativo propietario y diseñado exclusivamente para la naturaleza del tráfico de correo electrónico.

• **Un MTA Seguro** (Mail Transfer Agent, el "router" de email) que sea un producto no fácil de crackear. La mayoría de las soluciones de antispam / antivirus corren sobre MTAs de mercado (Postfix, Sendmail, etc) que son productos con serios problemas de seguridad. Aún cuando algunos de los softwares de MTA tienen más de 25 años en el mercado, Ironport Systems trabajó tres años a puertas cerradas en la creación de su propio MTA (esto fue para algunos de la competencia como "reinventar la rueda" y un trabajo inútil, pero hoy se demostró que la clave de una solución de seguridad de correo esta en su MTA). El MTA es la base de que todos los servicios que se monten encima puedan trabajar de forma correcta.

• **Un MTA de alta performance y escalable.** El MTA del Ironport tiene una capacidad de manejar hasta 10.000 conexiones concurrentes. Esto es cinco veces más rápido que cualquier MTA tradicional de mercado. El MTA del Ironport es capaz de enviar hasta 700.000 correos por hora.

• **Un MTA que controle correctamente las colas de envío y bounces.** Uno de los problemas más serios de los MTA de mercado es lo limitado que son en el manejo de colas de correo. Esto es un dolor de cabeza para los administradores. Los MTA tradicionales tienen una sola cola de envío, por lo tanto, cuando se "encolan" correos porque tienen que ir a un sitio (o dominio) que está lento y no salen, traban a todo el resto de los otros correos. También hay un ataque muy común que consiste en enviar múltiples correos a un sitio que serán rechazados por su servidor de correo (por ejemplo, el servidor de correo le envía un mensaje de retorno [bounce] que dice: casilla inexistente). Ahora bien, si le envío múltiples de estos mensajes a su servidor de correo, es probable que empiece a encolar y por lo tanto no puedan salir más correos de su plataforma. Es más, si el atacante es más dañino, le fraguará la dirección de retorno de modo que usted dirija estos mensajes de retorno a otra compañía. Esta compañía verá que esta siendo atacado por usted y lo reportará a un blacklist. ¿Le suenan familiares estos problemas? Seguramente sí y en algunos casos son causales no de una denegación total de servicio, sino de esas situaciones que suceden a diario que parece que el email anda lento, o se pierden correos o esas situaciones "raras" que luego parecen que se arreglan solas. No es así. Usted esta sufriendo este tipo de ataques a diario y probablemente no tenga siquiera visibilidad de ellas. El Ironport tiene un control total del manejo de bounces para evitar este tipo de ataques y las colas de envío son por dominio destino. Es decir, el Ironport crea tantas colas como dominios tiene para entregar. Luego tiene un sistema que las recorre secuencialmente. De este modo, si un dominio esta lento o caído, no perjudica al resto de los correos a enviar.

• **Sistema de protección contra ataques de directorio.** Una forma normal de descubrir los emails de las compañías es haciendo un ataque de directorio. De este modo, el atacante descubre por medio de "fuerza bruta" los nombres de email de la compañía. La forma que hace esto es enviando emails con nombres y esperando la respuesta de casilla inválida. De esta forma, el enviador se va equivocando de casillas e irá encontrando otras. La forma de solucionar esto es validar los usuarios en el perímetro de la red, conjuntamente con LDAP (o Active Directory) y contar con una herramienta capaz de detectar estos ataques. El Ironport es capaz de detectar estos ataques y bloquear a la IP del atacante de forma automática.

Es muy probable que si revisa su plataforma de correo actual cuente con solo algunos o ninguno de los puntos mencionados anteriormente. En general, la mayoría de los problemas de denegación de servicio de la plataforma de correo es debido a las causas que se mencionan anteriormente. Además el Ironport soluciona todo en un solo equipo, y su plataforma cambiará como se ve en la figura 1.

Antes de IronPort
Internet
Firewall
MTAs
Anti-Spam
Anti-Virus
Policy Management
Mail Routing
Servidor de Correo
Users

Despues de IronPort
Internet
Firewall
IronPort Email Security
Servidor de Correo
Users

Fig. 1

Protección Antispam

Probablemente haya escuchado y aprendido mucho sobre el tema antispam. Le habrán contado que los softwares antispam cuentan con filtros bayesianos, heuristicos, listas negras, listas blancas, etc; pero usted aún no se encuentra conforme porque el spam sigue pasando.
Los sistemas antispam tradicionales trabajan de forma reactiva, de igual forma que los antivirus. Es decir, primero el SPAM pasa y luego la empresa "escribe las reglas antispam" para el producto. Estos sistemas Antispam trabajan comúnmente analizando el contenido del mail, su envelope, su header, etc., y a partir de esto sacan una puntuación, dando como resultado de esta puntuación si el mensaje en cuestión es spam o no.
Este proceso de análisis de palabras, url, cadenas de caracteres, etc., tiene dos problemas importantes: a) es muy consumidor de recursos, por lo tanto hay que poner mucho hardware en caso de crecidas de spam, b) en el afán de dar una alta tasa de captura de spam son proclives a dar falsos positivos.
Ironport cuenta con dos modalidades de detección de spam: una proactiva y otra reactiva. La reactiva tiene un funcionamiento similar a lo mencionado anteriormente con la diferencia de que es un sistema adaptado a las nuevas tendencias de enviar spam (detección de URLs). Además, dado que la parte antispam proactiva se encuentra en primera instancia y es la que limpia cerca del 70 por ciento del tráfico de spam, este segundo análisis reactivo sólo hace una función de precisión en la detección de spam y no es el responsable de dar la alta tasa de detección, por lo tanto no da falsos positivos. También, a este segundo sistema antispam reactivo (se llama IPAS) como le llega poco tráfico no consume tantos recursos de CPU. Pasemos a explicar entonces, cómo funciona el primer sistema antispam (llamado Filtros de Reputación). Los filtros de reputación trabajan en conjunción con una base de conocimiento de IP enviadoras de correo, llamada Sender Base (www.senderbase.org).

Sender Base es un datacenter donde se alojan cerca de 200 servidores que colectan tráfico de correo a nivel mundial y es alimentado por los grandes proveedores de email (como ser Hotmail). También nos alimentan cerca de 50.000 empresas que colaboran con esta base y varios ISP del mundo entero (Ironport tiene como cliente a 8 de los 10 Top Ten ISP del mundo). Además, cada equipo Ironport instalado tiene la capacidad de alimentar esta base. Los parámetros de correo a los que se hace seguimiento en esta base son cerca de 110: IP, envelope, header, urls, archivos adjuntos, etc. Con estos datos, sabemos la naturaleza de envío de cada IP que manda correo en este mundo. Tenemos todas las zonas del mundo cubiertas ya que desde cualquier parte del mundo se envía correo a proveedores como Hotmail. Con estos datos obtenidos, acorde a su comportamiento de envío, calificamos a las IP entre -10 a +10. Siendo los negativos los malos enviadores y positivos los enviadores buenos. Pueden comprobar el listado de cualquier IP enviadora que conozcan, accediendo a www.senderbase.org y poniendo la IP a investigar (el número de calificación no lo verán desde Internet porque esto es propiedad intelectual de Ironport y es la clave del funcionamiento del producto).

La forma en la que funciona el primer sistema antispam (filtros de reputación) de la mano de Sender Base es la siguiente: un IP cualquiera inicia una comunicación SMTP con el Ironport. El Ironport hace una petición de Sender Base preguntando la calificación de la IP. Si la calificación es negativa, el Ironport corta la conexión. Es decir, el mail nunca entró en el equipo, ya a nivel de conexión es cortado. Este sistema tiene varias ventajas: la primera, se reduce el tiempo computacional ya que no se requiere analizar el contenido del correo. La segunda, por más ingenioso que sea el contenido del spam, como sabemos que esa IP esta siendo utilizada para enviar spam, eliminamos todo lo que proviene de ella. De aquí que es considerado un sistema proactivo. Con los filtros de reputación también detenemos las máquinas infectadas con virus que permanentemente intentan conectarse a nuestro sistemas de correo. Estas IP que son bloqueadas abruptamente son siempre máquinas Zombies (PC de usuarios de banda ancha que fueron infectadas y ahora son utilizadas para enviar SPAM). Hay muchas personas que se dedican a proveer máquinas infectadas, que ellos llaman "proxies" para enviar spam a través de ellas (si quieren descubrir estas empresas basta con que pongan "oculte su IP" en cualquier buscador de Internet y aparecerán varias de estas empresas que ofrecen métodos de este tipo para enviar spam). En síntesis, el 70 por ciento del spam es detenido en este sistema, que solo consiste en "cortar" comunicaciones TCP. Esta es la razón por la cual el Ironport es un equipo tan rápido y utilizado en los grandes ISP. Sin duda alguna, nuestra base de conocimiento "Sender Base" es clave en la calidad del producto.

Fig. 2

Otras Funcionalidades

Los productos Ironport también cuentan con un sistema Antivirus tradicional. El antivirus que integra Ironport es Sophos, uno de los antivirus más rápidos del mercado y una alternativa de perímetro distinta a lo que comúnmente existe en las PC de los usuarios.
Ironport cuenta con poderosos filtros que puede armar el administrador acorde a sus necesidades de análisis del contenido de los correos que pudieran entrar o salir de la empresa.
También los equipos cuentan con una poderosa herramienta de gestión, análisis y reporte, pudiéndose ver en tiempo real exactamente qué es lo que esta sucediendo en la plataforma.

Protección contra epidemias de Virus

Como se mencionó en el punto anterior, en Sender Base inspeccionamos qué tipos de archivos adjuntos se están compartiendo en Internet. Lo que hemos creado es un sistema de "alerta temprana" antes epidemias de virus, que funciona del siguiente modo: cuando vemos que un adjunto esta siendo compartido por muchas personas en Internet, lo más probable es que sea una nueva epidemia. El equipo Ironport consulta cada 5 minutos a Sender Base por si se ha detectado una nueva epidemia. Cuando aparece un nuevo adjunto que es una epidemia, el Ironport automáticamente crea un filtro que detiene ese adjunto y lo manda a una cuarentena especial en el disco interno. Este adjunto será retenido en esta cuarentena, hasta tanto el antivirus (sophos) que tiene el Ironport tenga la vacuna para analizarlo. Cuando el Antivirus tiene la vacuna adecuada, el Ironport automáticamente libera la cuarentena y deja que sea analizado por el AV. Con este sistema de alerta temprana que nos provee Sender Base hemos detenido epidemias de virus hasta 41 horas a que el primer vendor de antivirus tuvo la vacuna para la epidemia. Con este sistema minimizamos el tiempo de exposición del servidor de correo ante una nueva epidemia de virus.

Gestión de Seguridad de la Información

Una decisión Estratégica

Fabián G. Chiera
Gerente de la División
de Servicios Profesionales
ETEK Argentina

La ola de compliance de regulaciones locales y del exterior marca una tendencia en el corto y mediano plazo a la que las compañías en Argentina, también tendrán que sumarse. La ISO-IEC 27001:2005 es la base para el cumplimiento de todas estás regulaciones.



Introducción

Si bien aún en la Argentina las certificaciones de seguridad no son tomadas con la seriedad necesaria, es claro que en un futuro cercano poseer una certificación de seguridad será algo muy importante e incluso hasta obligatorio.

Las compañías hoy en día interrelacionan distintos sistemas (clientes, facturación, stock, sistemas on-line, etc.). Estos sistemas están avalados por contratos y SLAs (Service Level Agreements), pero ninguno de ellos establece claramente las responsabilidades de seguridad de una y otra parte, por lo cual, no son suficientes. Es imperativo asegurar el tratamiento adecuado de la información y la continuidad de negocio. Éste es el mejor SLA que podemos proveer a nuestros Clientes.

Los riesgos de seguridad aumentan día a día y las compañías cada vez están más expuestas. En forma más seguida se observan noticias que involucran pérdida de dinero debido a pérdida de información.

La interacción con transferencia de información entre las compañías es un hecho y la única forma de asegurarle a la otra compañía el manejo adecuado de los riesgos del tratamiento de la información es mediante un sistema de gestión de la seguridad de la información certificado. Un sistema de gestión de la seguridad de la información está diseñado con la finalidad de proporcionar controles de seguridad adecuadamente seleccionados. Por todo esto, **la adopción de una certificación de gestión de seguridad debe ser una decisión estratégica para la organización.**

El nuevo modelo propuesto por BSi (British Standard Institute) y adoptado por ISO bajo la denominación ISO-IEC 27001:2005 propone la implementación, operación y mejora de un sistema que provea un framework para el manejo seguro y ágil de la información. **"Seguro"** implica mantener niveles de riesgos adecuados para la organización, de acuerdo con sus objetivos, protegiendo la confidencialidad, integridad y disponibilidad de la información.

Este moderno sistema cambió mucho a su antecesor: la BS 7799-2. La ISO-IEC 27001:2005 es un sistema mucho más simple de gestionar. Un cambio muy importante es que la responsabilidad será explícita sobre los gerentes y directivos de la organización. Por ello, es que el framework propuesto por esta Norma es de muy fácil manejo y dirección.

Sistema de Gestión de la Seguridad de la Información

Un SGSI – Sistema de Gestión de la Seguridad de la Información (o sus siglas en inglés, ISMS – Information Security Management System) es un conjunto de mecanismos (directrices, registros, información, procesos, controles de seguridad) que son gerenciados, es decir, analizados, planificados, controlados, verificados, validados y en constante mejora continua. Un ISMS basado en ISO 27001:2005 es un sistema con aproximación a procesos, es decir, la seguridad de la información se basa en identificar los flujos de información entre distintos procesos.

El modelo Plan-Do-Check-Act define la gestión de la seguridad, es decir, el ISMS. Si observamos la ISO-IEC 27001:2005 en el punto 4.2, vamos a observar que este modelo de mejora continua (PDCA) se ve reflejado en la Norma (ver cuadro).

ISO 27001:2005	Correspondencia Modelo PDCA
4.2.1 – Establish de ISMS	Plan
4.2.2 – Implement and Operate de ISMS	Do
4.2.3 – Monitor and Review ISMS	Check
4.2.4 – Maintain and Improve de ISMS	Act

Implementación de un ISMS

El primer paso dentro del proceso del establecimiento de un sistema de gestión es definir su alcance. El alcance será determinado de forma estratégica para la organización. El mismo es un conjunto de procesos, estructura física, organigrama, información, entidades internas y externas, y redes de teleinformática. El alcance y los límites del sistema deberán ser definidos en características del negocio, la organización, su ubicación, activos y tecnologías, incluyendo los detalles y las justificaciones de las exclusiones del alcance.

Luego del establecimiento del alcance se deberá definir la política del ISMS. Esta política incluye un framework para establecer objetivos y la definición de la dirección y las acciones a tomar en función de la seguridad de la información. Deberá incluir también la identificación de todas regulaciones, leyes, reglamentos y estatutos que apliquen al ISMS. Asimismo, la política del ISMS establecerá los criterios para evaluar los riesgos.

Establecida la política del ISMS, se procederá con la definición de los procesos de evaluación de riesgos de los activos y se identificarán todos los activos con sus respectivas vulnerabilidades y amenazas. Toda esa información conformará la evaluación de riesgos. Habrá que determinar los mecanismos de tratamiento de aquellos riesgos que no sean aceptables para la organización. Asimismo, la identificación de los riesgos residuales y su tratamiento. El tratamiento de riesgos implica la selección de los objetivos de control y los controles de seguridad a implementar, además, del plan de mitigación que se aplicará. Estos análisis deberán ser aprobados explícitamente por el management.

Cuando se dispone de todo esto, se puede comenzar con el armado del SOA (Statement of Applicability). El SOA detalla todos los controles (según ISO-IEC 27001:2005 Anexo 'A') que aplican al ISMS. En el SOA además se deberán justificar todas aquellas exclusiones. Las exclusiones se producen cuando alguno de los 133 controles definidos en el Anexo A de la Norma no son aplicables al ISMS. Tengamos en cuenta que la ISO-IEC 27001:2005 define los controles mínimos a implementar, por lo cual las exclusiones deberán ser justificadas adecuadamente su no aplicabilidad.

Una vez completado estos pasos, estaremos en condiciones de comenzar a operar el sistema.

Recordemos que el sistema es en su mayor parte la identificación continua de nuevos riesgos y la evaluación de todos los riesgos en su conjunto, los definidos anteriormente y los nuevos. Por lo cual, la selección de la metodología de evaluación de riesgos es un componente crítico del sistema.

La operación del sistema se basará en gran parte en el manejo de incidentes. Los incidentes de seguridad representan una violación al sistema, es decir, que los controles que fueron aplicados no fueron suficiente, por lo cual, merecerá una nueva evaluación de riesgos para el activo de información que fue afectado por el incidente. ●

Sobre el Autor:

Fabián G. Chiera – Gerente de la División de Servicios Profesionales de ETEK Argentina. Es Implementador Líder de la Norma ISO-IEC 27001:2005, quien además dirige y acompaña a las compañías en su proceso implementación y certificación.

DFS

Sistema de Archivos Distribuido

DFS es la tecnología de Microsoft que permite, entre otras cosas, centralizar nuestros backups y simplificar la estructura de carpetas compartidas, logrando así la reducción de costos en, por ejemplo, nuestras oficinas de sucursal.

IT Pro en PyMEs

Por **Sebastián Passarini**
Administrador de Redes

Serie | Nota #3 de 5

La Empresas se fusionan, crecen, se expanden geográficamente. Algunas confían cada vez más sus procesos de negocio a otras empresas de outsourcing de servicios como ser servicios de IT y de RR.HH, entre otros. Es decir, el mundo se globaliza y es necesario para quienes quieran competir en este escenario, que todo esté conectado, compartiendo información y disponiendo de ella las 24 HS del día, los siete días de la semana. En función de esto, y debido a la falta de personal capacitado en tareas de IT en nuestras oficinas de sucursal, es que debemos implementar soluciones para que la administración de estos sitios remotos tienda a 0. Optimizar recursos aprovechando los enlaces de comunicaciones existentes será vital para poder cumplir el objetivo. Si lográramos realizar todos nuestros backups en las oficinas centrales por ejemplo, evitando así la manutención y compra de hardware de backup y de sus insumos para cada sitio, ¿no sería un ahorro importante de dinero? Es en este escenario donde podemos hacer uso de las tecnologías/servicios de Windows Server 2003 llamadas espacios de nombres DFS y replicación DFS, dependiendo esta última del servicio FRS (File Replication Service). Al configurar estos elementos estaremos obteniendo una solución completa para la administración de los archivos de la compañía tanto locales como remotos. Lo único necesario será un poco de ingenio y ganas de innovar. En el cuadro "uso combinado de DFS y FRS" podemos ver algunas de las ventajas que se obtienen con su implementación.

¿Cómo funciona esta tecnología?

En la figura 1 podemos observar cómo un equipo, en este caso un servidor de AD, es configurado como el servidor de "espacios de nombres DFS". Todo comienza con la creación de un "DFS root" (carpeta compartida principal), que a su vez contiene links (carpetas compartidas secundarias) quienes apuntan a los recursos compartidos reales (los targets), es decir, a los servidores donde se encuentran almacenados los datos. Para acceder a las carpetas compartidas de la compañía solo tenemos que conectar el DFS Root a una única unidad de red. De esta manera estamos creando un "espacio virtual" desde donde podemos acceder en forma centralizada a todos nuestros archivos ya sean estos locales o remotos.
Cuando un usuario necesita ingresar a un archivo de nuestra red, este se conecta a los links dentro de nuestro namespace (Punto 1 de la figura 1), los que a su vez están redireccionando al usuario sin que este se entere a la ubicación donde realmente se encuentran los archivos, es decir a los targets (Punto 2 de la figura 1).
Con el uso de esta tecnología también estamos eliminando gran cantidad de unidades de red con las que estamos acostumbrados/obligados a trabajar a diario (ver Figura 2).

Replicación DFS o Automática

Aquí tenemos el segundo componente de nuestro Sistema de Archivos Distribuido, el "Servicio de Replicación de Archivos o FRS", el cual agrega una nueva funcionalidad a nuestro espacio de nombres DFS. En el punto 3 de la figura 1 podemos observar cómo los targets 1 y 2 están replicados entre los servidores "Central" y "Sucursal", formando así un grupo

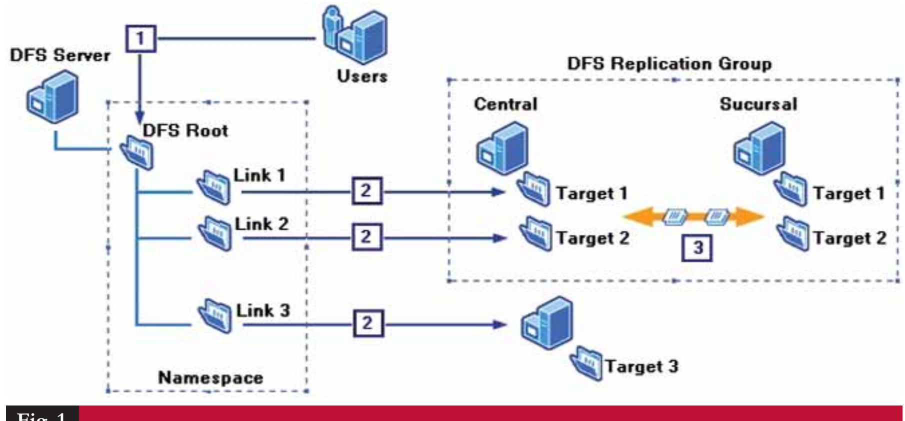


Fig. 1

de replicación DFS. Esto significa que quienes accedan a los Links 1 y 2 serán redireccionados a los servidores “Central” o “Sucursal”, según criterios que trataremos más adelante. También podemos notar cómo el link 3 no posee réplica, actuando sólo como un redireccionamiento de carpetas compartidas.

Uso combinado de DFS y FRS permite:

- ***Centralizar los backup de la compañía.***
- ***Limitar el tráfico de red sobre enlacen WAN lentos replicando solo los cambios entre archivos en lugar del archivo completo.***
- ***Que todos los sitios mantengan una copia actualizada de los documentos modificados sin importar desde qué sitio se realice esta modificación***
- ***Asegurar la disponibilidad de archivos aún cuando un servidor haya sufrido una caída inesperada.***
- ***Disminuir la cantidad de unidades de red necesarias para mapear carpetas compartidas ubicadas en distintos servidores.***
- ***Cambiar la ubicación de carpetas compartidas sin la necesidad de modificar scripts y sin que el usuario note diferencia alguna.***

Una vez configurada la replicación entre targets de un mismo link cada archivo que sea modificado y cerrado se replicará automáticamente a su espejo, es decir, el otro target. En la figura 3 vemos cómo luego de la modificación y cierre de archivos, estos son replicados en forma automática hacia sus espejos o targets de réplica, sin importar desde qué sitio hayan sido modificados. ¿Y si dos personas modifican el mismo archivo a la vez? En este caso el último en cerrar el archivo modificado gana. La replicación trabaja mediante el uso de un protocolo llamado RDC (compresión diferencial remoto), el que se encarga de replicar sólo los cambios realizados en los archivos en lugar de replicar el archivo completo, logrando optimizar el uso del ancho de banda en enlaces WAN lentos. Esto nos brinda una nueva posibilidad. Podremos liberar en las oficinas de sucursal a las personas que no son de IT y que hoy tienen entre sus tareas realizar y controlar los backups, permitiendo de esta manera que solo se dediquen a las labores que sus puestos de trabajo les demandan y, al unificar nuestros backups en las ofi-cinas centrales mediante del uso de la replicación de targets, estaremos logrando, entre otras cosas, el ahorro del dinero que hoy destinamos al hardware de respaldo e insumos en las oficinas de sucursal. Hasta aquí hemos visto que al modificar y cerrar un archivo este es copiado a su replica en forma automática, lo cual indica que puede ser un buen método para trabajar con archivos que deban ser consistentes en varios sitios a la vez, por ejemplo: procedimientos y planillas de cálculo.

Sin DFS	Con DFS
net use x: \\central\it	net use y: \\domain\dfs
net use m: \\sucursal\managers	
net use s: \\central\sales	

Fig. 2

Pero en caso que solo trabajemos con réplicas con el único objetivo de realizar backups nocturnos de nuestras sucursales en nuestras oficinas centrales, podemos schedulear las replicaciones para que se efectúen fuera del horario laboral y de baja utilización de los enlaces, logrando así realizar un único backup con toda la información de la compañía. Durante la configuración del servicio podremos seleccionar la topología a utilizar pudiendo elegir entre las siguientes:

- “Ring Topology”: los archivos se replican entre los equipos siguiendo un orden circular.
- “Hub and Spoke”: un servidor es designado como el hub server y el resto de los servidores (los spokes) solo pueden replicar contra este. Los archivos se replican desde el hub server hacia los spokes y viceversa, pero no puede haber replicación entre spokes.
- “Full mesh topology”: todos los servidores pueden replicar archivos con los demás.

Conmutación por recuperación del cliente

En la figura 4 y ahora sí en la práctica podemos ver la configuración de nuestro Sistema de Archivos Distribuidos desde la consola de administración de Windows Server 2003. Aquí vemos cómo el link “it” apunta a varios targets, es decir, que puede hacer referencia a varios servidores a la vez. De esta forma cuando un usuario quiera acceder a dicho link podrá ser direccionado a un target o al otro, dependiendo por lo general de: proximidad del servidor (sería lógico que los usuarios de un sitio determinado tengan como prioridad al target ubicado en las mismas instalaciones), imposibilidad de acceder a un target por caída del equipo, mantenimiento del mismo o interrupción del enlace de comunicaciones (ver \\sucursal2\it en figura 4).

Pero, ¿y si el servidor que funciona como DFS root ya no está disponible?

En la figura 2 “Con DFS” se observa cómo podemos conectar a una unidad de red nuestro DFS root, indicando el nombre de dominio en lugar del nombre del servidor. Si el servidor principal también llamado host server no llegase a estar disponible por alguna razón, los clientes intentarán conectarse a través de una réplica del DFS root ubicada en los restantes servidores de AD. Para lograr esto debemos publicar el DFS root en Active Directory y replicarlo a los otros servidores de Dominio

Configuración y Administración de los espacios de nombres DFS

Esto podemos hacerlo desde la consola de administración que se encuentra en “Programs\Administrative Tools\Distributed File System” o ejecutando “dfsgui.msc”. También podemos administrar nuestro servidor DFS desde el símbolo del sistema mediante el uso de los archivos de comando "Dfsradmin.exe", "Dfsrdiag.exe" y "Dfsutil.exe". Finalmente, si instalamos las herramientas de administración del cliente, podremos administrar DFS desde nuestros puestos de trabajo.

Factores que impiden la implementación de la Replicación DFS

Es posible que una vez configurado nuestro namespace nos topemos con el problema de que no podemos configurar las replicas entre targets o que las mismas no funcionan correctamente. En el cuadro “Consejos para una

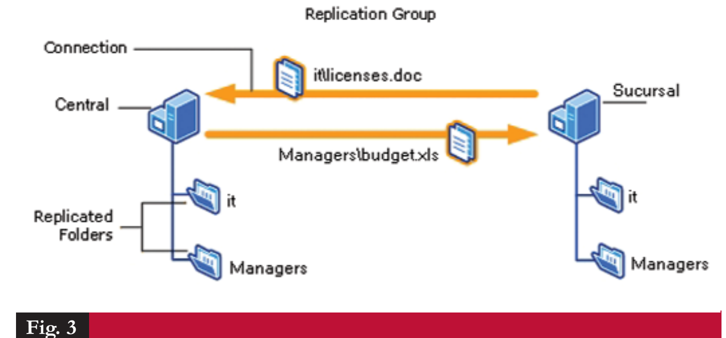


Fig. 3

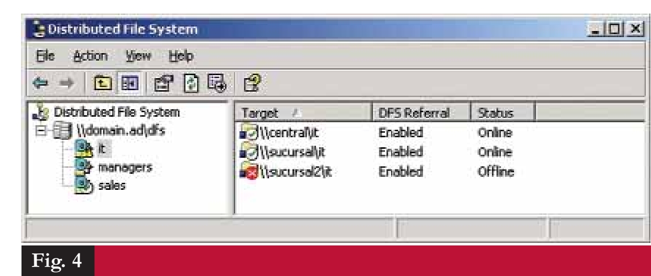


Fig. 4

buena implementación" podemos encontrar algunas sugerencias que nos ayudarán a evitar este tipo de problemas. Luego, y para quienes por algún motivo no puedan configurar la replicación entre targets existe otra solución, la que por su nombre, parece salida de película. Es el uso del comando "ROBOCOPY.EXE", el cual podemos obtener desde el kit de recursos de Windows Server 2003. Este comando toma como parámetros los recursos compartidos (los targets) "fuente" y "destino", y copia a "destino" solo las diferencias. Esta es una forma manual de replicar los archivos entre targets, y aunque resulta efectiva y tiene costo 0, tengan en cuenta que no replica archivos abiertos, es decir archivos que estén en uso por alguna aplicación al momento de intentar copiarlos.

Conclusión

Con la implementación de espacios de nombres DFS podemos lograr, entre otras cosas, simplificar la cantidad de unidades de red necesarias para acceder a nuestras carpetas compartidas, obtenemos tolerancia a fallos mediante el uso de links y sus targets, y ahorramos dinero con la administración centralizada de nuestros backups. Creo que son motivos suficientes para que cada uno de nosotros apostemos al cambio y comencemos con nuestros labs para evaluar estas tecnologías. Recuerden que nuestro presupuesto es acotado, motivo por el cual debemos explotar nuestros recursos y capacidades al máximo. ●

Links de Referencia

- http://www.google.com, buscar "Espacios de nombre DFS y Replicación DFS"
- http://www.microsoft.com/windowsserver2003/technologies/storage/dfs/default.mspx
- http://support.microsoft.com/kb/915146
- http://www.ss64.com/nt/robocopy.html

Lectura Adicional

"Mastering Windows Server 2003 – Mark Minasi" de SYBEX. Sin duda uno de los mejores libros acerca de Windows 2003, donde no solo encontrarán información acerca de este tema, sino que además podrán usarlo como guía para convertirse en verdaderos especialistas.

Concejos para una buena implementación

• Antes de replicar targets sería más que conveniente bajar a cada servidor una copia lo más actualizada posible del origen de los datos.
• Stand-alone DFS no soporta replicación DFS.
• La replicación DFS solo puede activarse entre servidores del mismo bosque de Active Directory.
• La replicación DFS no es aplicable entre archivos de gran tamaño y que cambian permanentemente como ser bases de datos Lotus Domino ó SQL.
• La replicación DFS no reemplaza a los backups.
• Servidores Windows 2003 sin sp1 pueden tener un comportamiento inconsistente. Se recomienda mantener los servidores con las últimas actualizaciones disponibles.
• El software antivirus debe ser compatible con la Replicación DFS.

Virtualización

Muy pocos saben o entienden hoy en día de qué se habla cuando se habla de Virtualización. En esta nota repasaremos sus conceptos básicos derribando mitos y dando a conocer sus verdades.

Autores:
Javier Cabral & Sebastián Cesario
SK Tecnología S.A.

En la actualidad el crecimiento de las empresas obliga a incrementar la cantidad de hardware en los centros de cómputos, incrementando así el caos diario del administrador de sistemas. Pero la poca homogeneidad en los datacenters no es el único problema que enfrenta la gente de IT, a veces las compras pueden llegar a tardar semanas o meses, no pudiendo así cumplir en tiempo y forma con las necesidades. Hoy en día, se empiezan a escuchar conceptos como consolidación o virtualización, pero cuando la gente habla de esto, ¿de qué habla realmente?

Hay diferentes formas de definir la Virtualización, y de clasificarla. En principio, la virtualización se refiere a una abstracción, es un paradigma que a pesar de ser la tendencia en la actualidad tiene sus orígenes en los años 60 con los primeros mainframes, donde el hardware y el software se independizan totalmente, y el hecho de tener una única máquina física no esta necesariamente atado a tener un solo servidor. La larga historia comienza por 1967 cuando IBM desarrolla el hypervisor, el cual se transformaría posteriormente en el VM del mainframe. En 1973 anuncian la S/370 modelo 158 y 168 que fueron las 2 primeras máquinas en realizar particionamiento físico. Ya para 1987 IBM había desarrollado el particionamiento lógico en el mainframe (Figura 1). La historia continuó en el año 1999 con el particionamiento lógico donde aparece esta tecnología en los procesadores RISC de arquitectura POWER con los primeros sistemas iSeries (ex AS/400) de IBM y evolucionó al día de hoy donde podemos ver cómo en el servidor más pequeño de una sola unidad de altura (p5-505Q) y un diseño ultra-denso podemos tener decenas de sistemas operativos corriendo en forma simultanea.

Esto último es tomando como ejemplo la arquitectura POWER de IBM en la cual nos estaremos basando para ejemplificar la tecnología de virtualización. Cada fabricante y cada implementación de esta tecnología tiene sus variantes y peculiaridades. Hay aplicaciones que implementan parte de la funcionalidad de un hypervisor por software y de esta manera permiten ejecutar múltiples sistemas operativos y virtualizar recursos de forma similar pero en arquitecturas completamente diferentes.

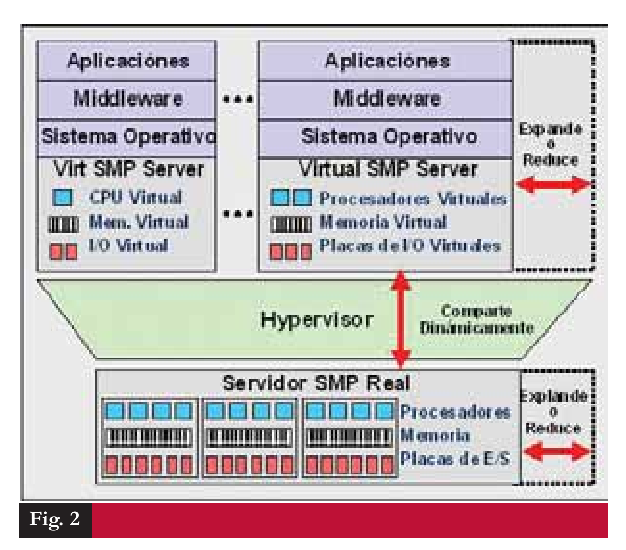


Fig. 2

¿Para qué sirve esta tecnología y qué ventajas ofrece?

Esta tecnología trae aparejados muchos beneficios para el sector de IT ya que sirve para poder reutilizar los recursos, particionándolos, de modo de correr múltiples sistemas operativos en un mismo hardware, compartiendo recursos físicos y de esta forma contando con menos cantidad de hardware ocioso.

Por otro lado, el hecho de que estas "máquinas virtuales" compartan la máquina real, no significa que estén dependiendo una de la otra. El hypervisor (Figura 2) se encarga de distribuir los recursos multiplexando las solicitudes de procesamiento de cada partición mediante un dispatcher que se encuentra implementado por firmware. Por otro lado los recursos de E/S se pueden asignar a cada partición de forma física y dedicada, o se pueden virtualizar al 100 por ciento. En este último caso la virtualización de recursos de E/S, como ser las placas de fibra, SCSI, Ethernet y discos se encuentra controlada por el VIO Server que es una capa delgada de software que gerencia las solicitudes de recursos virtualizados.

La virtualización trae consigo un concepto de encapsulamiento y aislamiento que es el que permite garantizar la integridad y seguridad de las operaciones que se realicen en las distintas particiones. A modo de ejemplo cada partición corre su propio sistema operativo, son su propio kernel y los dispositivos físicos que ve cada partición son reales y dedicados, o virtualizados y compartidos. En este último caso la partición accede a una imagen del recurso físico que es un dispositivo virtual que el VIO Server mapea al recurso físico correspondiente pero cada partición ve sus dispositivos como propios y dedicados, mas allá de lo que suceda por arriba del hypervisor.

Un ejemplo de cómo se comparten los recursos adquiridos entre distintos ambientes y sis-

System z
z/OS | Linux | z/VM
PR/SM Hypervisor
Servidor z/990

POWER: Llevando la tecnología System z a UNIX, Linux e i5/OS
AIX | Linux | i5/OS
POWER Hypervisor
Servidor POWER5

Fig. 1

temas operativos es el siguiente. Un caso típico: el disco rígido interno requerido para el sistema operativo. Hoy en días todos los discos traen al menos 36GB de espacio, y en cada uno podemos alojar más de 1 sistema operativo. ¿Por qué adquirir entonces un disco para cada partición cuando puedo optimizar el uso de los mismos y tener en un solo disco de 36GB el sistema operativo para 4 particiones?! Descontando que si quiero redundancia para espejar los discos del sistema operativo puedo tener 2 discos en lugar de 8!

Eso mismo puedo hacer con las placas de red, contar con un puerto 10/100/1000 pero optimizar el uso del mismo para darle servicio a varias particiones para salir a la red externa. De la misma forma con placas de fibra para SAN (Redes de almacenamiento) y placas SCSI. Otro gran beneficio de esta tecnología se ve cuando necesito armar un nuevo ambiente de pruebas para una nueva aplicación que quiero implementar.

Con la virtualización puedo poner en marcha un nuevo ambiente en cuestión de minutos tomando los recursos físicos que necesite de mi ambiente actual. Para hacer eso en un ambiente sin virtualización ni particionamiento tendría que sacar un poco de memoria física de un servidor que no la estuviera utilizando, un poco de disco interno de un segundo servidor que le sobre disco interno, un poco de procesador de un tercer servidor que le sobra algo de CPU y por ultimo un pedazo de un backplane de un cuarto servidor que le sobra ancho de banda en su bus interno de datos.

Suena un poco difícil de implementar, pero eso es exactamente lo que se hace en un ambiente virtualizado. Y no se hace una única vez, ya que las cargas de trabajo van fluctuando y varían a lo largo del tiempo y de los minutos y segundos. Todo este movimiento de recursos se puede hacer en forma dinámica. Puedo dinámicamente poner y sacar procesador, poner y sacar memoria, disco y placas internas de acuerdo a mis necesidades de carga de trabajo en cada momento.

Beneficios para el negocio

Hoy en día el crecimiento de las empresas lleva a traer nuevas aplicaciones y adquirir cada vez más máquinas, las cuales pueden no aprovechar sus recursos de manera eficiente pero tienen que existir ya que diferentes aplicaciones no siempre pueden convivir en un mismo entorno de OS. Esto trae consigo un inevitable desperdicio de hardware. ¿Qué pasaría si pudiéramos tirar todos los recursos que tenemos en una mesa y tomar de ahí lo que se necesite para cada aplicación en cada momento? Seguro sobrarían recursos y siempre algo quedaría en la mesa en un momento dado.

Esta nueva tecnología permite hacer exactamente esto, reducir de manera drástica el TCO (Total Cost of Ownership) de las soluciones ya que se necesita menos hardware para correr los mismos sistemas ya que se utilizan los recursos de manera más eficiente.

Para sacarle provecho a la Virtualización no hay que pensarlo solo como una tecnología, sino como una plena estrategia de negocios, imaginar un ambiente donde dos aplicaciones corren en diferentes horarios. Supongamos una aplicación online con su pico de utilización durante el día y una aplicación batch que corre durante la noche, en una situación normal se requerirían dos servidores para correr dichas aplicaciones, pero esta tecnología nos permite que un mismo hardware albergue en dos particiones ambas aplicaciones, y asigne los recursos en el momento adecuado, y cuando no, se los asigne a la partición que lo necesite.

El ejemplo más sencillo es el de la aplicación crítica, que tiene un pico de procesamiento a fin de mes. Con la virtualización al cierre del mes puedo dar más recursos a la partición que contiene el aplicativo pero seguir garantizando el aislamiento con el resto de las particiones. Puedo reutilizar el hardware de ese servidor montando en él nuevas particiones y sistemas operativos y de esta manera no comprometer la carga de trabajo de mi aplicación crítica. Sería inviable si voy a tener un ambiente de pruebas y testing conviviendo bajo un mismo sistema operativo pero con la tecnología de virtualización puedo garantizar a mi aplicación los recursos que necesita cuando los necesita sin riesgo alguno.

Tipos de Virtualización

En la actualidad la virtualización ofrece diversas posibilidades, las que van desde la virtualización a nivel de hardware hasta el nivel de software. A su vez hay dos maneras de virtualizar hardware. La primera es teniendo recursos físicamente encapsulados dentro de la arquitectura hardware donde cada set de recursos puede albergar una partición. La segunda, ve los recursos hardware como un todo y los controla, asigna y desasigna de acuerdo a la configuración y la necesidad a través de una entidad de orden superior en el firmware, que controla los recursos y obedece a reglas y turnos de uso que se encuentran previamente definidos. Esta segunda forma de virtualización en el caso de IBM también permite asignar placas PCI de forma física y dedicadas, permitiendo un mix entre los dos tipos de virtualización de ser necesario. IBM ofrece la solución más robusta en este tipo de Virtualización, debido a su gran cantidad de años de Know-How virtualizando main-

Mitos y verdades sobre Virtualización

¿Compartir los recursos trae consigo overhead?

Sí, es cierto, el hecho de compartir CPU puede traer overhead. En cualquier situación que se compartan recursos puede haber demoras inevitables, como por ejemplo las cajas en un supermercado. Pero es un mito que esto haga imposible el trabajo ya que siguiendo con el mismo ejemplo, esta tecnología permite que estando en la caja 1, podamos pasar parte de la mercadería por la caja 2 y otro tanto por la caja 3. Seria como tirar todos los productos en un gran canasto (Hypervisor) que se va a encargar de pasar cada uno por la caja que se libere primero. Es por esto que lejos de apreciarse una degradación de performance producto de la tecnología misma, lo que se observa es un considerable aprovechamiento de los recursos y una normalización de las cargas de trabajo. Claro que si configuramos mal un servidor y lo dimensionamos equivocadamente vamos a tener overhead como con cualquier otra tecnología, pero esta tecnología probó a través del tiempo que el overhead dejó de ser un limitante y hoy ya es un tema resuelto. Hoy en día las soluciones están muy optimizadas al punto de no percibirse un problema asociado a la misma tecnología que se esta impulsando.

¿Qué pasa si una partición cae o necesita reiniciarse?

La virtualización es una solución contemplada para empresas, donde como todos sabemos, el downtime se paga muy caro en términos del negocio, por eso, es una solución pensada para que cada ambiente actúe independientemente del otro. La pregunta correcta en este caso seria qué tanto necesito reiniciar mi partición debido a la virtualización, y la respuesta a eso esta atada a la solución que ofrece cada vendor, y es uno de los puntos mas críticos donde fijarse a la hora de elegir una solución de este tipo.

¿La virtualización es accesible a cualquier empresa o es solo una solución de High End?

Hay diferentes tipos de soluciones en el mercado de acuerdo al porte de las empresas y a la criticidad en cuanto a disponibilidad y performance de su trabajo, con lo cual es una tecnología totalmente accesible si se elije correctamente. La solución en principio disminuye el TCO, con lo cual si se ve como una estrategia de negocios plantea importantes ahorros y simplificación en la estructura de IT.

¿La virtualización es solo para servidores?

No, aunque esta nota intenta enfocarse solo en los servidores hoy en día se encuentra bastante difundida en diferentes áreas de tecnología, como son servidores, storages, centrales telefónicas y hasta estaciones de trabajo entre otras. Sus grandes prestaciones, su simpleza y la reducción de costos que propone la hacen atractiva para su uso en muchos campos de la tecnología.

2006

Jornada de marketing y desarrollo en internet

Dattatec.com, una vez más, nutre a la comunidad de webmasters, diseñadores web y desarrolladores, organizando e invitándolos a una jornada completa con el mix exacto de marketing y desarrollo para alcanzar el éxito de los proyectos en internet.

Más información e inscripción en:
http://www.dattatec.com/evento301106

ROSARIO | 30 **NOVIEMBRE** 2006
Hotel Ariston - Salón Perseo

Sorteo de productos Microsoft al finalizar el evento



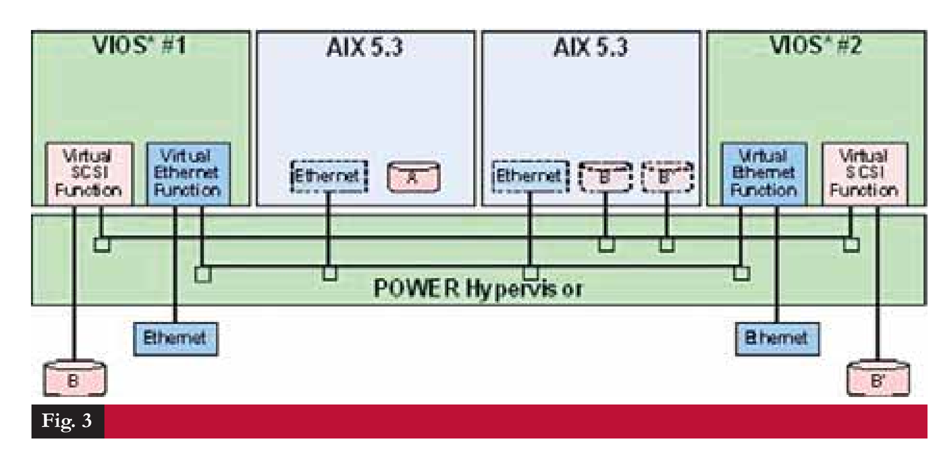


Fig. 3

frames, estructura por demás probada en este aspecto. A nivel de software, las soluciones consisten en un sistema operativo base sobre el cual se crean particiones, de manera que este OS se encarga de asignar recursos y establecer sus pautas de uso.
Tanto a nivel de soft como de hard, existe dependiendo del fabricante la posibilidad de virtualizar de igual modo periféricos.

Ventajas del particionamiento

La definición de partición es la capacidad de que un servidor se comporte como dos o más servidores independientes. De esta manera, podemos tener dentro de un mismo servidor incluso diferentes distribuciones y versiones de sistemas operativos, como por ejemplo, un i5OS(OS400), un AIX y un Linux., de este modo tenemos las siguientes ventajas:
_Consolidación de los servidores
_Mantenimiento de servidores independientes
_Creación de un entorno de prueba mixto
_Ejecución de clústeres integrados

Oferentes en el Mercado

Como era de esperarse en el mercado hay gran cantidad de ofertas sobre Virtualización, pero las empresas de tecnología van evolucionando y madurando a diferentes ritmos de acuerdo a sus políticas y a sus capacidades.
En el mercado UNIX, HP, Sun e IBM ofrecen alternativas de Virtualización, las cuales aunque pueden ser a la vista bastante similares tienen sustanciales diferencias entre si. En principio las tres soluciones virtualizan a través de hardware, pero hay que prestarle atención a sus capacidades, a la granularidad, es decir, la fragmentación que puedo hacer del hardware (por procesadores y memorias enteros, por bancos de ellos o por fragmentos de los mismos), a la robustez de su arquitectura hardware, y a la manera en que maneja los downtime, ya que algunas plataformas pueden alocar recursos dinámicamente y otras no. En el mercado Windows en cambio, Microsoft y VMWare tienen una solución que procura ser en principio más homogénea, ya que ofrecen Virtualización a nivel de software. Tanto IBM como VMWare ofrecen soporte para LINUX.

Cómo darse cuenta si usted es un potencial cliente de virtualización

¿Usted tiene...
...aplicaciones que usan múltiples sistemas operativos?
...que manejar una infraestructura compleja?
...que saber qué cargas de trabajo corren en cada Server?
...un ambiente donde lidia con picos de cargas de trabajo?
...que hacer espacio y reordenar sus aplicaciones cada vez que necesita un nuevo ambiente de testing o desarrollo?

Servidor de Entradas/Salidas Virtuales (Virtual IO Server)

El VIO Server es un concepto utilizado por IBM el cual permite, definiéndolo en una partición lógica dentro de la máquina, lograr una abstracción de los recursos físicos utilizados, permitiendo:
• Compartir recursos físicos de E/S entre particiones del sistema
• Crear particiones sin necesidad de añadir más recursos de E/S físicos
• Crear más particiones que el número de ranuras de E/S o dispositivos físicos disponibles, con la posibilidad de que las particiones dispongan de E/S dedicada, E/S virtual o ambas
• Maximizar el uso de los recursos físicos del sistema
• Ayudar a reducir la infraestructura de la red LAN y SAN (Red de área de almacenamiento)
Para ambientes que requieren mayor disponibilidad se pueden configurar Virtual I/O Servers redundantes (ver figura 3).
Se utiliza para virtualizar recursos físicos tales como placas ethernet, placas Fiber Channel, discos internos, etc. Es común virtualizar todos los recursos en los servidores más pequeños ya que tienen menos capacidad de expansión de placas y de discos físicos. Para esto existe una versión del Virtual I/O Server llamada el IBM Virtualization Manager. Este es un VIO Server integrado en el servidor con una interfaz web muy amigable al usuario que sirve para configurar y administrar las distintas particiones sin necesidad de adquirir una consola física de administración. Conocida como HMC o Hardware Management Console (ver figura 4). ●

Sobre los Autores

Lic. Javier Cabral Bettitelli - Consultor Especializado en Tecnologías Unix (AIX, HP-UX, Linux) y Storage High End. Se desempeño trabajando en consultoría unix como asociado de negocios de HP e IBM Argentina. Cuenta con 5 Certificaciones de IBM (4 de ellas en tecnologías POWER) y una certificación del Linux Professional Institute.

Sebastián Cesario - Consultor Unix especialista en diferentes plataformas (AIX, HPUX, Solaris, LInux) y productos de comunicaciones de Cisco. Se desempeñó trabajando como administrador Unix en diferentes empresas y en proyectos de outsourcing para USA en IBM.

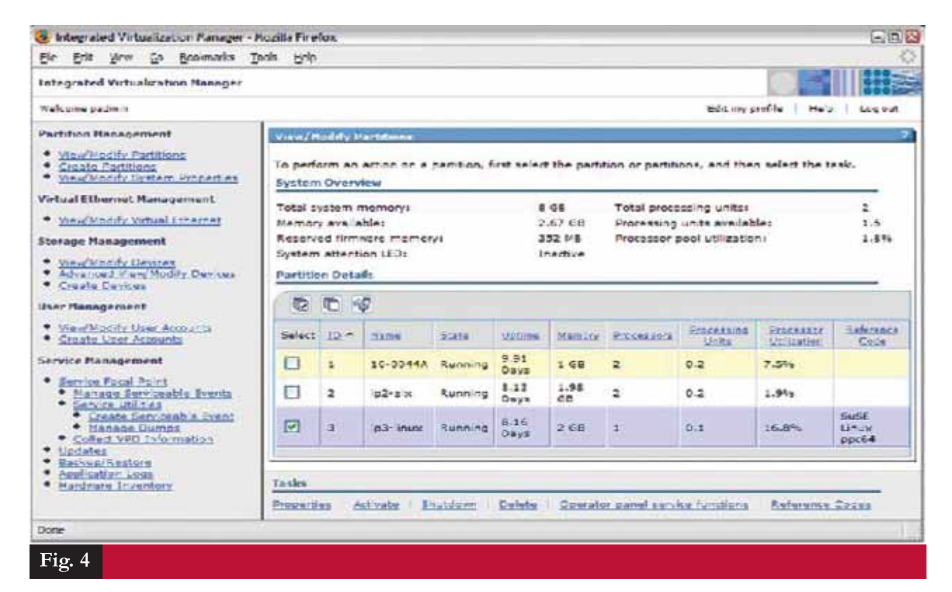


Fig. 4

¿Qué hay de nuevo para el diseño de Aplicaciones Web?

ASP.NET

ASP.NET hace posible el desarrollo de Sitios y Servicios Web XML. La nueva versión 2.0 de Microsoft .NET incluye mejoras en casi todas las áreas: diseño, productividad, seguridad, rendimiento, alojamiento, etc. En este artículo veremos cómo utilizar la "Master Page" la cual nos permite realizar "Herencia Visual" (un concepto nuevo de ASP .Net).



Gabriela Marina Giles

- *Microsoft .NET Senior Trainer* *CentralTech GOLD CERTIFIED Partners*
- *Presidenta de Desarrollador@s* *Grupo de usuarios de Tecnologías .NET* *www.desarrolladoras.org.ar*



Nota #3 de 6

Todos sabemos que los sitios Web en sus páginas tienen banners, controles y algún menú en común. En versiones anteriores de ASP.NET creábamos "User Control" para no copiar y pegar HTML específico de interfase "común" en las páginas del sitio Web. Es decir, creábamos el menú del sitio en un control de usuario para luego utilizarlo en las nuevas páginas que íbamos agregando al sitio. No teníamos forma de crear una plantilla donde definir todo lo que debería verse en cada página nueva.
Ahora en ASP.NET 2.0 podemos crear páginas que nos servirán como plantilla en nuestro sitio Web. Podremos definir los header, footer, menú, banners, etc. Esto nos permitirá realizar cambios de forma rápida y automática, ya que cualquier cambio que realicemos en la MasterPage será reflejado en aquellas páginas que la utilicen. También podemos agregar controles ASP (Server Control) y código del lado del servidor para esos controles, todo esto estará disponible en el resto de las páginas aspx que utilicen nuestra plantilla. Además podremos acceder a los atributos de la Master Page y crear nuevas propiedades si fuera necesario.
Otra ventaja importante es que tendremos soporte en diseño WYSIWYG (lo que ves, es lo que obtienes), es decir, lo que vemos en la edición será lo que veamos en el navegador.

¿Cómo funciona la MasterPage?

La MasterPage dispone de una estructura que contendrá elementos (Contenedores) llamados "*ContentPlaceHolder*" los cuales podremos sobrescribir en las **Páginas hijas** (que heredaran de la página maestra) pero manteniendo la estructura definida en la **MasterPage**. Para ilustrar su funcionamiento veamos la figura 1, en la cual definiremos una interfase con cabecera (header), contenido (Conten PlaceHolder) y un pie de página (footer).
Luego de definir la MasterPage para poder visualizar nuestro diseño debemos agregar una nueva página e indicar con qué MasterPage trabajaremos, como lo muestra la figura 2.
Entonces, por una lado las Masters definen **<asp: ContentPlaceHolder>** el lugar permitido para modificar en las páginas hijas y en estas a su vez definen un **<asp:Content>** que contendrá los ContenPlaceHolder que hayamos agregado en la página maestra (figura 3).
Si observamos el "Source" del Master Page (el texto plano generado) obtendremos el Cuadro 1. Como podemos observar en el código, el archivo empieza con la directiva **@Master** que simplemente le indica al motor de **ASP .NET** que este archivo definirá la estructura de una página.
El archivo **masterPage.master** dispone de elementos como el <head>, <body> y <form> donde podremos agregar tanto elementos **HTML** como **componentes de servidor de ASP.NET**.
Además podemos observar en la **página maestra**, definida en el código de arriba, un elemento de servidor llamado **asp: ContentPlaceHolder**, en el cual se podrá agregar elementos **HTML** y **elementos de servidor de ASP.NET** en las nuevas páginas hijas. Estos elementos serán heredados por las **Páginas hijas** del esquema y su contenido podrá ser reescrito en ellas usando el nombre asignado en el archivo **.master**. En la figura 4 vemos el código generado en "default.aspx" (página hija) que trabaja con la masterPage definida previamente.



Fig. 1

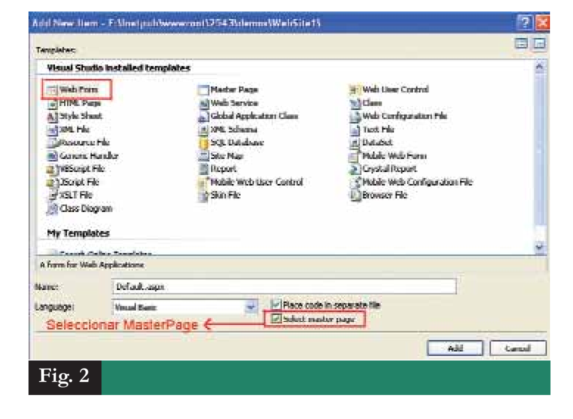


Fig. 2

```
<%@ Master Language="VB" CodeFile="MasterPage1.master.vb"
Inherits="MasterPage1" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
<head runat="server">
    <title>Untitled Page</title>
</head>
<body>
    <form id="form1" runat="server">
    <div>
        <asp:contentplaceholder id="ContentPlaceHolder1"
runat="server">
        </asp:contentplaceholder>
    </div>
    </form>
</body>
</html>
```

Cuadro 1

En la directiva **@Page** de la página default.aspx se ha especificado el nuevo atributo **"MasterPageFile"** el cual describe el archivo "master Page.master" del cual se tomará la estructura del sitio.

Observemos el elemento **asp:Content** (Figura 4) que usaremos para contener el asp:ContentPlaceHolder definido en el archivo masterPage.master. En el podremos modificar y reescribir su contenido agregándole elementos que puede ser código HTML o controles de servidor de ASP.NET. Para aplicar el masterPage en todo el sitio deberemos modificar el archivo Web.Config como se muestra en el siguiente código:

```
<configuration>
 <system.web>
 <pages masterPageFile="~/masterPage.master" />
  </system.web>
</configuration>
```

También podemos aplicar una masterPage mediante código:

```
void Page_PreInit (Object sender, EventArgs e)
{
    Page.MasterPageFile = "~/masterPage.master";
}
```

Para acceder a las propiedades de la xxx.master desde las páginas hijas utilizaremos la propiedad: **Page.Master**

La propiedad **Master** devuelve el objeto **MasterPage** asociado a la página. Esta es una propiedad de sólo lectura, también podemos establecer nuevas propiedades en el objeto MasterPage.

En el siguiente código en C# definimos una propiedad llamada "Nombre" desde la master page. El código escrito a continuación define la propiedad en el mismo diseño **masterPage.master**, lo que se conoce como **"código en línea"**. El script <script language="C#" runat="server"> representa el código que escribiríamos en el "CodeFile ="MasterPage.master.cs" si quisiéramos separar el diseño del código que se ejecutara del lado del servidor.

```
<asp:Label ID="Nombre" runat="server" />
…
…
<script language="C#" runat="server">
public string Nombre
{
    get { return txtNombre.Text; }
    set { txtNombre.Text = value; }
}
</script>
```

Para poder consumir la propiedad creada en la página maestra desde cualquier página xxx.aspx que contenga el atributo "MasterPageFile", escribiremos el siguiente código: Código en C#

```
Master.Nombre = "desarrolladoras.org.ar";
```

También podemos combinar el diseño de nuestra **MasterPage** con otras nuevas características, como por ejemplo los **"Themes y Skins"**. Los "THEMES" son grupo separado de archivos (Skin) que permiten descomponer la información de estilo y diseño. Un Skin es un conjunto de atributos visuales para uno o más controles que se define en un archivo con extensión .skin, esto no reemplaza al CSS sino que trabaja en conjunto. Un **Theme** puede aplicarse a cualquier sitio de forma tal que afecte la apariencia, el entorno y los controles del mismo. Todos los cambios en el Estilo de un sitio pueden administrarse realizando cambios en el Theme, sin necesidad de editar las páginas de forma individual. Los controles soportan **"Cascading Style Sheets" (CSS)** y un modelo de objeto Style para establecer las propiedades de estilo como fuentes, bordes, colores de fondo, altura, etc.

Podemos definir la información de los estilos como propiedades de los "CSS" o podemos definir esta información en "Theme", especificando en los "Skin" los estilos de controles individuales dentro de un "Theme". Para definir un THEME agregamos una carpeta App_Themes en nuestro sitio y luego definimos los temas (figura 5) y sus Skins (Figura 6). ●

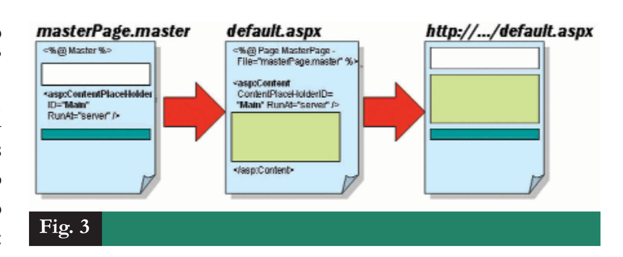


Fig. 3



Fig. 4

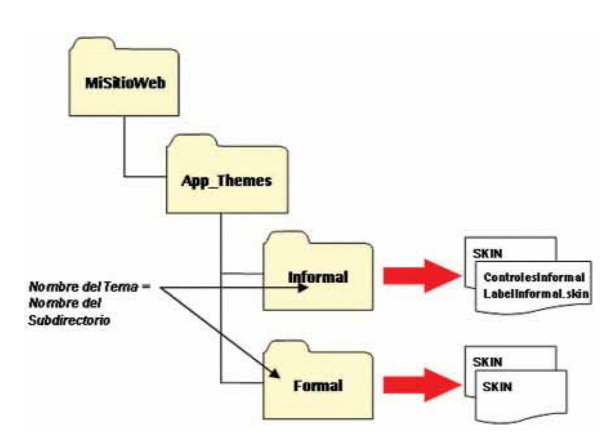


Fig. 5

App_Themes/Th...kinFile.skin*

```
<asp:Label runat="server" BackColor="Red" BorderColor="White"
        Style="position: relative" Text="Label"></asp:Label>
<asp:Label runat="server" CssClass="ColorEstilo" Style="left: -38px;
      position: relative; top: 32px" Text="Label"></asp:Label>
```

Este Skin está utilizanso una hoja de estilos

Fig. 6

Página	`<%@ Page Theme="Formal" @%>`

Código	`void Page_PreInit (Object sender, EventArgs e)`
	`{`
	`    Page.Theme = "Informal";`
	`}`

Todo el sitio	`<configuration>`
	`  <system.web>`
	`    <pages theme="Informal" />`
	`  </system.web>`
	`</configuration>`

Cuadro 2 Definición de temas THEMES

Usar Temas para Personalizar un Sitio
http://www.es-asp.net/tutoriales-asp-net/tutorial-61-106.aspx

MasterPage (Clase)
http://msdn2.microsoft.com/es-es/library/system.web.ui.masterpage.aspx

ASP.NET Themes and Skins Overview
http://msdn2.microsoft.com/en-us/library/ykzx33wh.aspx

Applying Styles, Themes, and Skins
http://quickstart.developerfusion.co.uk/QuickStart/aspnet/doc/themes/default.aspx

Themes and Skins in ASP.NET 2.0
http://www.codeguru.com/vb/vb_internet/aspnet/article.php/c7937/

Grupo de usuarios de tecnologías .NET:
www.desarrolladoras.org.ar

towebs®
Webhosting

Tome el control de su Website

Por que elegirnos:

:: Atención online y telefónico las 24hs.
:: Datacenter propio.
:: Más de 10.000 websites confían en nosotros.
:: Exclusivo sistema de chat online.



UNIX 100

:: Recursos

- 100 megabytes en disco.
- 20 cuentas de email pop3.
- Alias ilimitados.
- Autoresponders ilimitados.
- Panel de Control Personal 2.1!
- Cgi-bins, Perl y Java scripts.
- 2 Gb de transferencia mensual.
- 1 Redireccionamiento
- 1 cuenta FTP, SSH.

14[95]



UNIX 700

:: Recursos

- 700 megabytes en disco.
- 200 cuentas de email pop3.
- Alias ilimitados.
- Autoresponders ilimitados.
- Panel de Control Personal 2.1!
- Cgi-bins, Perl y Java scripts.
- 10 Gb de transferencia mensual.
- Redireccionamientos ilimitados.
- 25 cuentas FTP, SSH.

24[00]



NT 100

:: Recursos

- 100 megabytes en disco.
- 20 cuentas de email pop3.
- Alias ilimitados.
- Autoresponders ilimitados.
- Panel de Control Personal 2.1!
- Cgi-bins, Perl y Java scripts.
- 2 Gb de transferencia mensual.
- 1 Redireccionamiento.
- 1 cuenta FTP.

24[95]



Tel: +54 (11) 5031-1111

Av. Belgrano 1586, piso 10 - info@towebs.com - http://www.towebs.com

BREVES

Laptop de U$D100

Seguridad de vanguardia



El proyecto de una Laptop de U$D100 del Massachusets Institute of Technology Media Lab (MIT) es tan revolucionario si lo miramos desde los bajos costos como de las innovaciones en la seguridad.
Uno de los más importantes cambios es que estas computadoras van a emplear como sistema operativo a Linux, memoria flash en vez de un disco duro y un microprocesador que aunque es lento para los requerimientos actuales necesita de muy poca energía para funcionar. A esto se le suma el hecho de que programadores ya han diseñado protocolos de seguridad que esperan superen los conocido hasta el momento en el mercado informático. Si bien aun están testeando esta nueva propuesta creen que esta innovación en seguridad volverá innecesario el uso de softwares anti-virus en las laptops. Esta Laptops le exigirán a cualquier aplicación a correr en un "jardín amurallado" limitando el acceso a los archivos.
Y aunque la seguridad pueda llegar a fallar, una tecnología de encriptación especial va a prevenir que el BIOS (el software que corre en una computadora cuando es inicialmente encendida) sea sobrescrito.









El ministro de Educación, Ciencia y Tecnología Daniel Filmus y el presidente de la Cámara de Empresas de Software y Servicios Informáticos (CESSI) Carlos Pallotti presentaron la Campaña de Difusión de Carreras Informáticas denominada Generación TI, destinada a difundir las carreras universitarias vinculadas a las tecnologías de la información a nivel nacional.
El secretario de Políticas Universitarias, Alberto Dibbern explicó que "en el contexto del Plan Estratégico de Software y Servicios Informáticos 2004-2014, el Ministerio desarrollará proyectos destinados a promover, mejorar y fortalecer la formación en informática a nivel técnico y superior y financiará las actividades que realicen las universidades nacionales para el mejoramiento y actualización de la formación de técnicos universitarios". Esto se debe a que según un relevamiento realizado por la CESSI este año la demanda de técnicos y profesionales del sector no está cubierta por la escasa cantidad de recursos humanos que se forman, y que no existe una adecuada oferta de tecnicaturas de pregrado y de cursos de capacitación para el sector. Dibbern concluyó explicando que "la demanda en el año 2006 se calcula en más de 6000 técnicos y profesionales, con un curva ascendente que prevé llegar a 10.000 en 2010".



KASPERSKY INDEPENDIENTE

Luego de que Microsoft lanzara en junio OneCare, un software antivirus y antispam con el que pretende competir con los principales fabricantes del segmento, la cofundadora de Kaspersky Labs afirmó que el nuevo Windows Vista no dificultará el trabajo de las soluciones de seguridad de terceros fabricantes.
Esta es la primera opinión a favor de Microsoft. Tanto McAfee como Symantec, otras proveedoras de herramientas de seguridad, acusaron a la empresa de Bill Gates de dificultar la convivencia entre sus aplicaciones y el nuevo Windows Vista, denegando el acceso al kernel del sistema operativo.
Natalya Kaspersky concluyó que habrá que esperar uno o dos años para ver cómo se posiciona la solución de Microsoft en el mercado y qué tipo de competencia puede suponer realmente.



6ta Jornada del Software Libre

Entre el 13 y el 15 de octubre se desarrolló en la Universidad de Mendoza la **6ta Jornada del Software Libre**, un encuentro que reúne a entusiastas y seguidores del software libre de la región y que cuenta con la participación de panelistas y conferencistas de destacada trayectoria internacional. Desde el año 2000 que se realizan estas jornadas y este año en particular de la mano de LUGmen, el grupo de usuarios de GNU/Linux de Mendoza.
Para más información: *http://jornadas.lugmen.org.ar*

Humor - *Por Severi*




mundodelsoporte.com
9
Si la Asistencia Técnica se le ha hecho "cuesta arriba",
piense en la única red de servicio Independiente,
Profesional y a Escala en la región.
Muchas empresas han utilizado como herramienta de Marketing figuras emblemáticas del Deporte.
Ahora bien ... alguna de ellas, lo ha invitado a Ud. a jugar en Vivo y en Directo con esas Megaestrellas ?
Sólo el Mundo del Soporte lo hace posible.
Participe de la Clínica y Torneo PROAM, "Gánele a Los Cóceres" (Andrés, José, Juan Carlos, Ricardo y Roberto) y a otros Profesionales de Elite, a realizarse en el mes de Diciembre de 2006.
Salga en la línea con alguno de ellos.
El Mundo del Soporte
A Member of SupportLand Network
Bases y Condiciones en www.mundodelsoporte.com
Sea un Partner Oficial